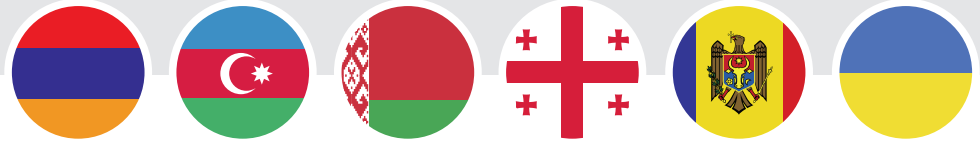
EU2017.EE

EaP Eastern Partnership

eGA e-governance academy 15 YEARS Empowering e-governance around the world

Рекомендации по безопасности и защите в киберпространстве и по э-демократии



ESTONIA DEVELOPMENT COOPERATION

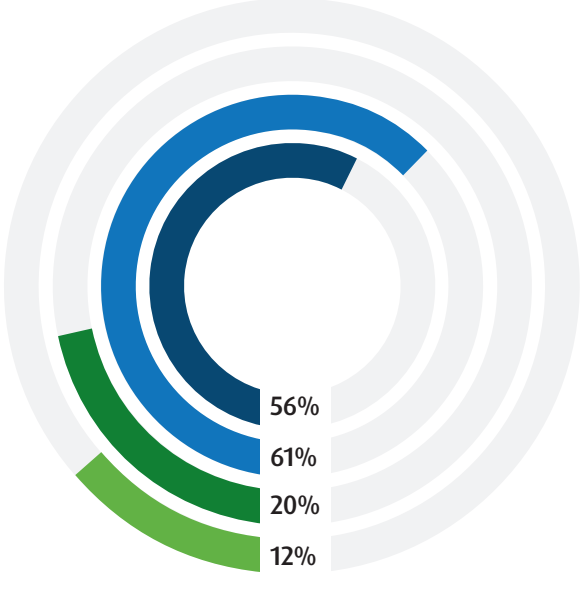
SWEDEN

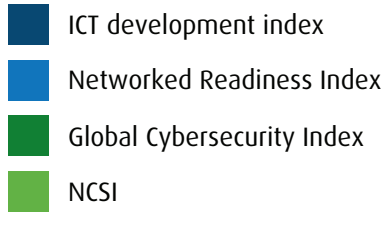
Рекомендации по безопасности и защите в киберпространстве

Армения

Относительно общего развития ИКТ (информационно-коммуникационные технологии), Армения выполнила 56% Индекса развития ИКТ (2016). Это ставит Армению на 71 место. Согласно Индексу Сетевой Готовности (2017), Армения выполнила 61% от максимальных критериев. Это ставит Армению на 56 место в Индексе. Оба эти Индекса показывают, что общее развитие ИКТ в Армении находится на уровне выше среднего.

Относительно развития кибер-безопасности, Индекс Глобальной Кибер-безопасности (2017) показывает, что Армения выполнила 20% критериев. Это ставит Армению на 110 место в мире. Наше исследование (NCSI) показывает, что Армения выполнила 12% критериев по кибер-безопасности.





В общем, это означает, что разрыв между ИКТ и кибер-безопасностью относительно большой. Армения уделяла внимание развитию ИКТ, но сейчас ей также необходимо уделить внимание развитию кибер-безопасности.

Существует хороший прогресс в сфере борьбы с кибер-преступностью, где Армения выполняет 60% критериев. Армения криминализировала кибер-преступления и имеет подразделение цифровой криминалистики и контактный пункт 24/7 для международных кибер-преступлений.

В дополнение, существует прогресс в сферах развития базовой безопасности и электронной подписи. Армения имеет ведомство по защите персональных данных и правовую среду для электронной подписи. Такое позитивное развитие следует продолжать..

В общем, кажется, что Армения нуждается в более полном и систематическом подходе к развитию национальной кибер-безопасности. Было бы хорошо организовать сначала стратегическое управление кибер-безопасностью, а после этого уделять внимание развитию секторального качества.

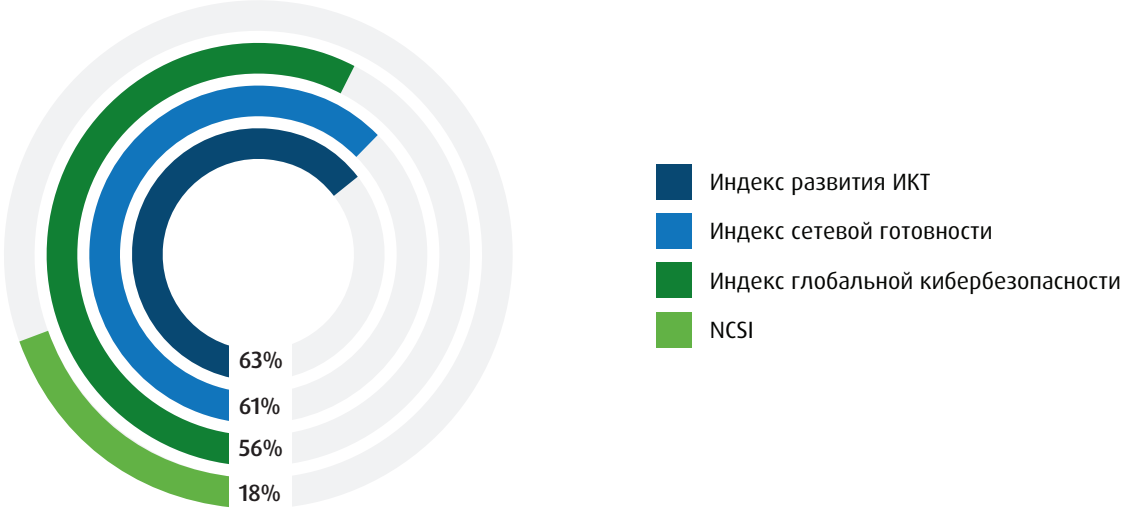
	Максимальный потенциал, %	12.12%
I	ОБЩИЕ ИНДИКАТОРЫ	
1.	Разработка концепции для защиты киберпространства	0%
2.	Понимание и анализ кибер-угроз	0%
3.	Образование и профессиональное развитие в сфере кибербезопасности	0%
4.	Международное сотрудничество в области кибербезопасности	10%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ	
5.	Основной стандарт кибер- и информационной безопасности	27%
6.	Безопасная среда для э-услуг	0%
7.	Электронная идентификация и электронная подпись	25%
8.	Защита критически важных э-услуг и инфраструктуры критичной информации	0%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ инцидентами И КРИЗИСОМ	
9.	Способность управления кибер- инцидентами	0%
10.	Способность управления широкомасштабными кибер-кризисами	0%
11.	Борьба с кибер-преступностью	60%
12.	Способность проводить операции национальной обороны	0%

Ситуация по кибер-безопасности Армении в соответствии с NCSI.

Азербайджан

Относительно общего развития ИКТ, Азербайджан выполнил 63% Индекса развития ИКТ (2016). Это ставит Азербайджан на 58 место в Индексе. Согласно Индексу Сетевой Готовности (2017), Азербайджан выполнил 61% от максимальных критериев. Это ставит Азербайджан на 53 место в Индексе. Оба эти Индекса показывают, что общее развитие ИКТ в Азербайджане находится на уровне выше среднего.

Относительно развития кибер-безопасности, Индекс Глобальной Кибер-безопасности (2017) показывает, что Азербайджан выполнил 56% критериев. Это ставит Азербайджан на 48 место в мире. Наше исследование (NCSI) показывает, что Азербайджан выполнил 18% критериев по кибер-безопасности..



В общем, это означает, что разрыв между развитием ИКТ и кибер-безопасностью существует и Азербайджану нужно уделять больше внимания развитию кибер-безопасности.

Существует хороший прогресс в сфере анализа кибер-угроз, где Азербайджан выполнил 75% критериев. В дополнение, сфера электронной идентификации и электронной подписи является относительно хорошо развитой (50%).

Из таблицы мы также можем видеть, что существует некоторый прогресс в области управления кибер- инцидентами (44%), в области международного сотрудничества (30%), в области образования по кибер-безопасности (20%), в области борьбы с кибер-преступлениями (10%) и в области основной безопасности (9%).

В общем, существует много сфер кибер-безопасности, которым Азербайджану нужно уделять внимание с целью поддержания хорошего развития сферы ИКТ. Кажется, что Азербайджан нуждается в более полном и систематическом подходе к развитию национальной кибер-безопасности. Было бы хорошо организовать сначала стратегическое управление кибер-безопасностью, а после этого уделять внимание развитию секторального качества.

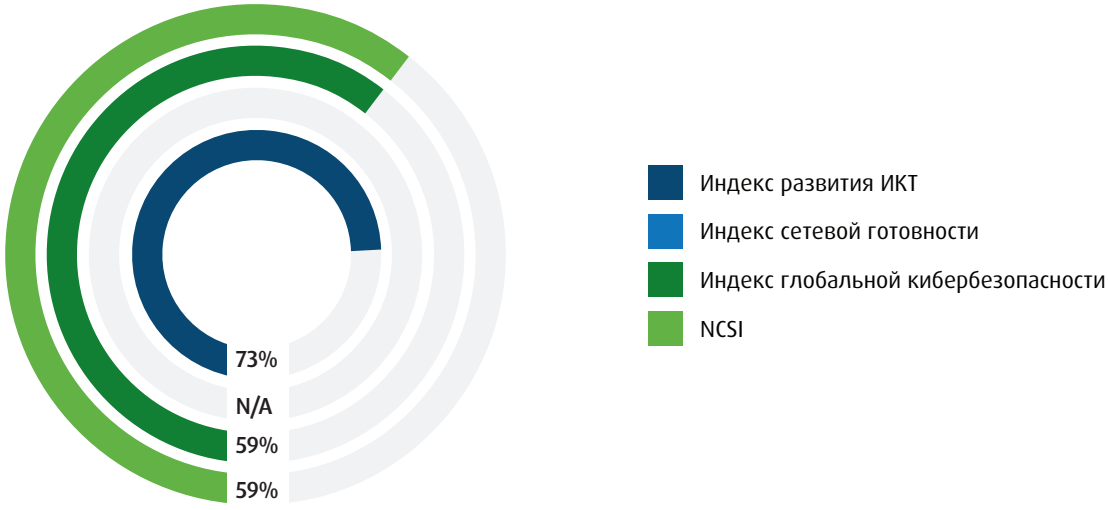
	Максимальный потенциал, %	18.18%
I	ОБЩИЕ ИНДИКАТОРЫ	
1.	Разработка концепции для защиты киберпространства	0%
2.	Понимание и анализ кибер-угроз	75%
3.	Образование и профессиональное развитие в сфере кибербезопасности	20%
4.	Международное сотрудничество в области кибербезопасности	30%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ	
5.	Основной стандарт кибер- и информационной безопасности	9%
6.	Безопасная среда для э-услуг	0%
7.	Электронная идентификация и электронная подпись	50%
8.	Защита критически важных э-услуг и инфраструктуры критичной информации	0%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ инцидентами И КРИЗИСОМ	
9.	Способность управления кибер- инцидентами	44%
10.	Способность управления широкомасштабными кибер-кризисами	0%
11.	Борьба с кибер-преступностью	10%
12.	Способность проводить операции национальной обороны	0%

Ситуация по кибер-безопасности Азербайджане в соответствии с NCSI.

Беларусь

Относительно общего развития ИКТ, Беларусь выполнила 73% Индекса развития ИКТ (2016). Это ставит Беларусь на 31 место Индекса. Это показывает, что общее развитие ИКТ в Беларуси очень хорошее.

Относительно развития кибер-безопасности, Индекс Глобальной Кибер-безопасности (2017) показывает, что Беларусь выполнила 59% критериев. Это ставит Беларусь на 39 место в мире. Наше исследование (NCSI) показывает, что Беларусь выполнила 59% критериев по кибер-безопасности.



В общем, развитие кибер-безопасности в Беларуси находится на уровне выше среднего (59% от максимума). Тем менее, принимая во внимание тот факт, что развитие ИКТ намного выше (73% от максимума), больше внимания необходимо уделять кибер-безопасности.

Существует четыре сферы, где Беларусь получил максимальные оценка 100%. Этими сферами являются (6.) безопасная среда для э-услуг, (7.) электронная идентификация и электронная подпись, (8.) защита критически важных э-услуг и инфраструктуры критичной информации, и (9.) способность управлять кибер- инцидентами.

Наименее развитыми сферами являются: (10.) Управление широкомасштабными кибер-кризисами, (4.) международное сотрудничество в области кибер-безопасности и (1.) развитие политики. Беларусь принимала участие в мероприятиях по международному управлению кибер-кризисом, но испытывает недостаток в производственных возможностях страны в целом для управления кибер-кризисом. В дополнение, Беларусь нуждается в прогрессе в сфере международного сотрудничества. Например, Беларусь не внедрила Конвенцию Европейского Суда по кибер-преступлениям.

Относительно развития кибер-политики, Беларусь имеет координационный формат, не имеет специализированного подразделение для разработки политики. В дополнение, Беларуси не хватает терминов и определений по кибер-безопасности, стратегии по национальной кибер-безопасности и плана внедрения национального уровня..

В общем, ситуация по кибер-безопасности Беларуси относительно хорошо развита и этот хороший прогресс требует перехода на более высокий уровень.

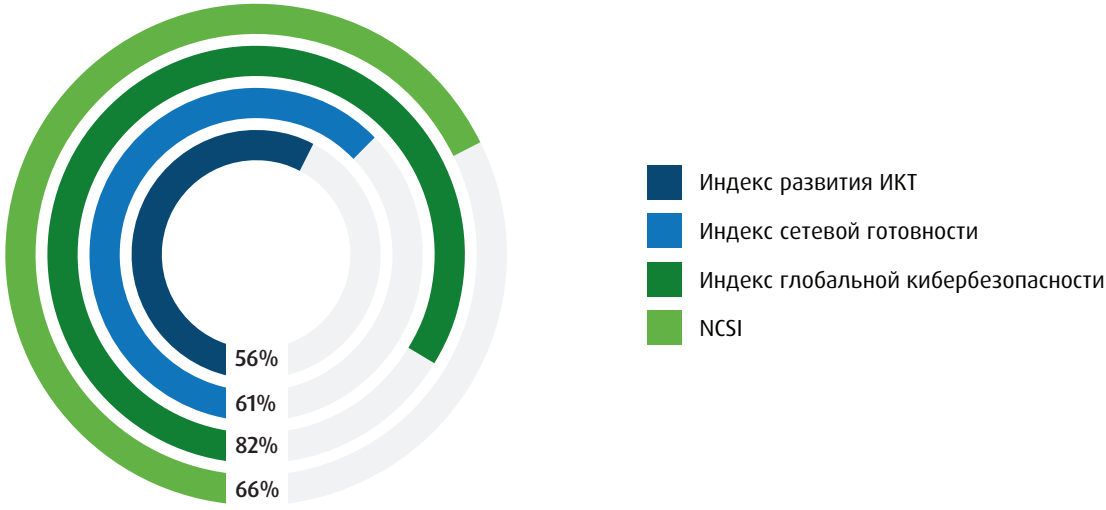
	Максимальный потенциал, %	59.09%
I	ОБЩИЕ ИНДИКАТОРЫ	
1.	Разработка концепции для защиты киберпространства	25%
2.	Понимание и анализ кибер-угроз	75%
3.	Образование и профессиональное развитие в сфере кибербезопасности	55%
4.	Международное сотрудничество в области кибербезопасности	20%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ	
5.	Основной стандарт кибер- и информационной безопасности	55%
6.	Безопасная среда для э-услуг	100%
7.	Электронная идентификация и электронная подпись	100%
8.	Защита критически важных э-услуг и инфраструктуры критичной информации	100%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ инцидентами И КРИЗИСОМ	
9.	Способность управления кибер- инцидентами	100%
10.	Способность управления широкомасштабными кибер-кризисами	11%
11.	Борьба с кибер-преступностью	60%
12.	Способность проводить операции национальной обороны	60%

Ситуация по кибер-безопасности Беларуси в соответствии с NCSI.

Грузия

Относительно общего развития ИКТ, Грузия выполнила 56% Индекса развития ИКТ (2016). Это ставит Грузию на 72 место в Индексе. Согласно Индексу Сетевой Готовности (2017), Грузия выполнила 61% от максимальных критериев. Это ставит Грузию на 58 место в Индексе. Оба эти Индекса показывают, что общее развитие ИКТ в Грузии находится на уровне выше среднего.

Относительно развития кибер-безопасности, Индекс Глобальной Кибер-безопасности (2017) показывает, что Грузия выполнила 82% критериев. Это ставит Грузию на 8 место в мире. Наше исследование (NCSI) показывает, что Грузия выполнила 66% критериев по кибер-безопасности..



Грузия является одной из немногих стран, где развитие кибер-безопасности лучше развития ИКТ. С точки зрения кибер-безопасности, ситуация очень хорошая. В настоящий момент необходимо обдумать, как сбалансировать развитие кибер-безопасности с развитием ИКТ.

Грузия получил максимальные оценка (100%) в пяти областях: (1.) разработка концепции, (2.) понимание и аналитика кибер-угроз, (7.) электронная идентификация и электронная подпись, (8.) защита основных э-услуг и инфраструктуры критичной информации, и (11.) борьба с кибер-преступлениями. Очень хорошо, что централизованно важные активности, такие как разработка концепции и анализ угроз имеют максимальные показатели. Это демонстрирует, что потенциал для развития сбалансированной безопасности является высоким.

В дополнение, (9.) сфера управления происшествиями, (6.) безопасная среда для э-услуг и (5.) основная кибер-безопасность развиты относительно хорошо. Сферами, которые больше всего нуждаются во внимании, являются: (3.) образование в сфере кибер-безопасности, (12.) способность к кибер-защите, (4.) международное сотрудничество и влияние и (10.) управление крупномасштабными кибер-кризисами.

В общем, мы можем сказать, что в Грузии очень хорошо организован национальный уровень кибер-безопасности. Несмотря на тот факт, что существуют некоторые сферы, которым необходимо внимание, вся кибер-безопасност в Грузии хорошо организована.

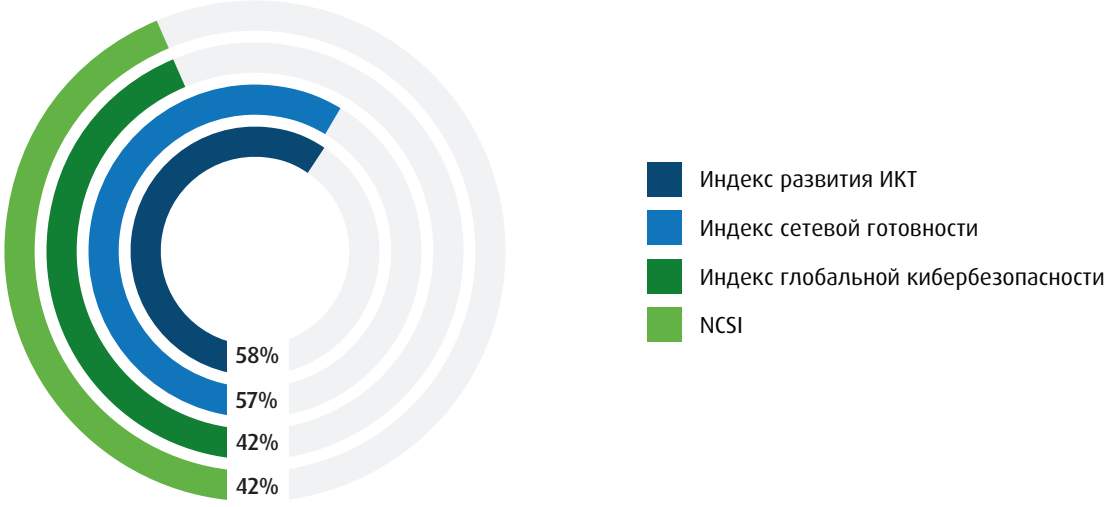
	Максимальный потенциал, %	65.66%
I	ОБЩИЕ ИНДИКАТОРЫ	
1.	Разработка концепции для защиты киберпространства	100%
2.	Понимание и анализ кибер-угроз	100%
3.	Образование и профессиональное развитие в сфере кибербезопасности	20%
4.	Международное сотрудничество в области кибербезопасности	40%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ	
5.	Основной стандарт кибер- и информационной безопасности	64%
6.	Безопасная среда для э-услуг	75%
7.	Электронная идентификация и электронная подпись	100%
8.	Защита критически важных э-услуг и инфраструктуры критичной информации	100%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ инцидентами И КРИЗИСОМ	
9.	Способность управления кибер- инцидентами	89%
10.	Способность управления широкомасштабными кибер-кризисами	33%
11.	Борьба с кибер-преступностью	100%
12.	Способность проводить операции национальной обороны	20%

Ситуация по кибер-безопасности Грузии в соответствии с NCSI.

Республика Молдова

Относительно общего развития ИКТ, Молдова выполнила 58% Индекса развития ИКТ (2016). Это ставит Молдову на 68 место в Индексе. Согласно Индексу Сетевой Готовности (2017), Молдова выполнила 57% от максимальных критериев. Это ставит Молдову на 71 место в Индексе. Оба эти Индекса показывают, что общее развитие ИКТ в Молдове находится на уровне выше среднего.

Относительно развития кибер-безопасности, Индекс Глобальной Кибер-безопасности (2017) показывает, что Молдова выполнила 42% критериев. Это ставит Молдову на 72 место в мире. Наше исследование (NCSI) показывает, что Молдова также выполнила 42% критериев по кибер-безопасности.



Молдова совершила знаменательное развитие в сферах (6.) безопасной среды для э-услуг, (7.) электронной идентификации и электронной подписи и (11.) борьбы против кибер-преступлений. Во всех этих сферах Молдова получила 100% максимального уровня.

В дополнение, основная кибер-безопасность является в Молдове относительно хорошо развитой (73% максимума). Молдова имеет ведомство по защите персональных данных, законодательство для классификации информации, минимальные требования для кибер-безопасности и требования для аудита системы ИКТ. Важная возможность состоит в том, что в настоящий момент Молдова не имеет ответственного ведомства по кибер-безопасности. Это очень важная возможность, которая требует развития в близком будущем.

Сферами, где Молдова совершила некоторый прогресс, являются: (1.) разработка концепции, (3.) образование, (4.) международное сотрудничество и (9.) управление кибер-инцидентами. Молдова имеет национальную программу по развитию кибер-безопасности (стратегия) и план внедрения. То, что требуется в сфере развития политики - это управление и координация.

	Максимальный потенциал, %	42.42%
I	ОБЩИЕ ИНДИКАТОРЫ	
1.	Разработка концепции для защиты киберпространства	38%
2.	Понимание и анализ кибер-угроз	0%
3.	Образование и профессиональное развитие в сфере кибербезопасности	30%
4.	Международное сотрудничество в области кибербезопасности	10%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ	
5.	Основной стандарт кибер- и информационной безопасности	73%
6.	Безопасная среда для э-услуг	100%
7.	Электронная идентификация и электронная подпись	100%
8.	Защита критически важных э-услуг и инфраструктуры критичной информации	0%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ инцидентами И КРИЗИСОМ	
9.	Способность управления кибер- инцидентами	56%
10.	Способность управления широкомасштабными кибер-кризисами	0%
11.	Борьба с кибер-преступностью	100%
12.	Способность проводить операции национальной обороны	0%

Ситуация по кибер-безопасности Молдове в соответствии с NCSI.

Относительно образования, Молдова имеет веб-сайт кибер-безопасности и несколько видов деятельности по информированию общественности. Допол-нительно, Молдова имеет программу кибер-безопасности на уровне бакалавриата. В будущем Молдова нуждается в том, чтобы больше внимания уделять общему образованию по кибер-безопасности в школах, а также профессиональному развитию.

Относительно управления происшествиями, Молдова имеет Правительственную Оперативную Группу по Компьютерным Происшествиям 24/7. В то же время в Молдове отсутствует законоположение, которое делает обязательной информирование о кибер-инцидентах. В дополнение, Молдова нуждается в том, чтобы уделять внимание созданию формата для государственно-частного сотрудничества.

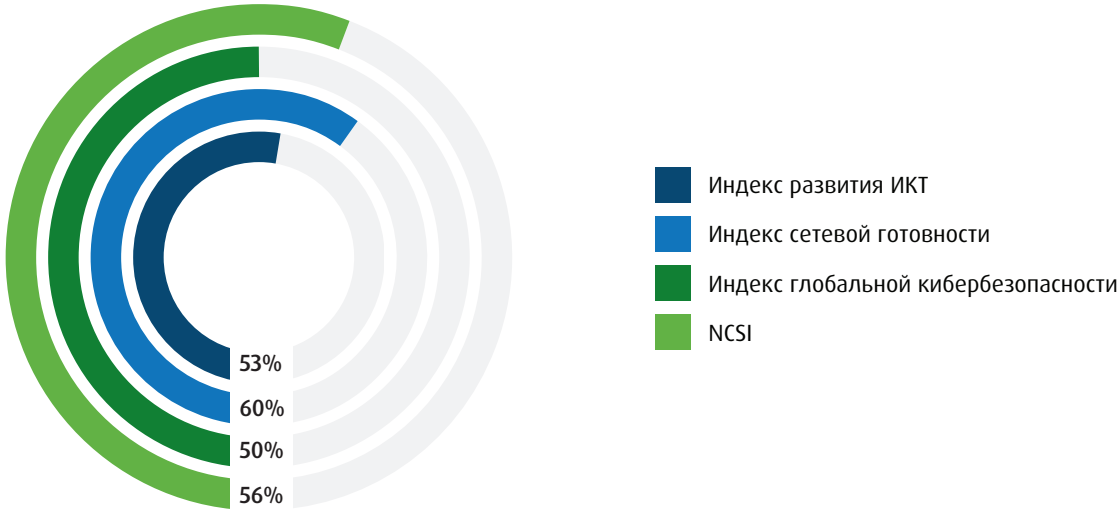
В большей степени Молдова нуждается в развитии в следующих областях:
(2.) анализ кибер-угроз, (8.) защита критически важных э-сервисов и инфраструктуры критичной информации, (10.) способность управлять крупномасштабными кибер-кризисами и (12.) потенциал национальной защиты.

В общем, кажется, что Молдова нуждается в более полном и систематическом подходе к развитию национальной кибер-безопасности. Было бы хорошо организовать сначала стратегическое управление кибер-безопасностью, а после этого уделять внимание развитию секторального качества.

Украина

Относительно общего развития ИКТ, Украина выполнила 53% Индекса развития ИКТ (2016). Это ставит Украину на 76 место в Индексе. Согласно Индексу Сетевой Готовности (2017), Украина выполнила 60% от максимальных критериев. Это ставит Украину на 64 место в Индексе. Оба эти Индекса показывают, что общее развитие ИКТ в Украине находится на уровне выше среднего.

Относительно развития кибер-безопасности, Индекс Глобальной Кибер-безопасности (2017) показывает, что Украина выполнила 50% критериев. Это ставит Украину на 58 место в мире. Наше настоящее исследование (NCSI) показывает, что Украина выполнила 56% критериев по кибер-безопасности.



В общем, развитие ИКТ и кибер-безопасности в Украине находятся приблизительно на том же уровне. С точки зрения кибер-безопасности, баланс между этими областями хороший. Это следует учитывать при развитии цифрового общества.

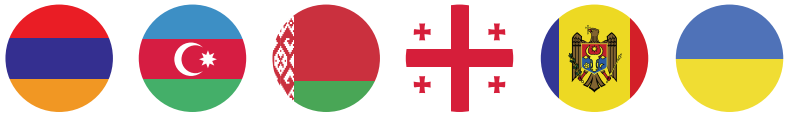
Существует пять видов активности, которые очень хорошо развиты в Украине. К ним относятся: (11.) борьба с кибер-преступлениями, (1.) разработка концепции, (5.) основная кибер-безопасность, (7.) электронная идентификация и электронная подпись и (3.) образование в сфере кибер-безопасности. В этих сферах Украина получила 75-90% максимального оценка.

Менее развитыми сферами являются: (2.) понимание и анализ кибер-угроз, (12.) возможность национально кибер-защиты, (4.) международное сотрудничество, (6.) безопасная среда для э-услуг и (10.) способность управлять широкомасштабными кибер-кризисами.

Существует много областей, где Украина нуждается в развитии специфичной и секторальной способнпсть кибер-безопасности. Анализ кибер-угроз и распространение информации среди широкой публики, бизнес- и публичного сектора определенно являются теми способнпстями, которые нуждаются в том, чтобы держать их в фокусе. Это сделает общество более сильным и подготовленным к кибер-происшествиям. Активность национальной кибер-защиты - это другая сфера, которая нуждается в значительном развитии.

	Максимальный потенциал, %	56.06%
I	ОБЩИЕ ИНДИКАТОРЫ	
1.	Разработка концепции для защиты киберпространства	88%
2.	Понимание и анализ кибер-угроз	0%
3.	Образование и профессиональное развитие в сфере кибербезопасности	75%
4.	Международное сотрудничество в области кибербезопасности	20%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ	
5.	Основной стандарт кибер- и информационной безопасности	82%
6.	Безопасная среда для э-услуг	25%
7.	Электронная идентификация и электронная подпись	88%
8.	Защита критически важных э-услуг и инфраструктуры критичной информации	67%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ инцидентами И КРИЗИСОМ	
9.	Способность управления кибер- инцидентами	67%
10.	Способность управления широкомасштабными кибер-кризисами	33%
11.	Борьба с кибер-преступностью	90%
12.	Способность проводить операции национальной обороны	0%

Ситуация по кибер-безопасности Украине в соответствии с NCSI.



Общие рекомендации для Стран Восточного Партнерства

В качестве общего принципа, развитие кибер-безопасности в стране должно быть приблизительно на одном уровне с развитием ИКТ. Если страна заинтересована в развитии цифрового общества, страна должна уделять равное внимание кибер-безопасности.

Эти области должны быть сбалансированы. Следующая таблица представляет общий обзор об ИКТ стран Восточного Партнерства и развития кибер-безопасности и показывают разрыв между областями.

Общий обзор относительно ИКТ стран Восточного Партнерства и Развития Кибер-Безопасности.

% макс. уровня ОНУНО	Армения	Азербайджан	Беларусь	Грузия	Молдова	Украина
Развитие ИКТ	58.5%	62%	73%	58.5%	57.5%	56.5%
Индекс развития ИКТ	56%	63%	73%	56%	58%	53%
Индекс сетевой готовности	61%	61%	N/A	61%	57%	60%
Развитие кибербезопасности	16%	37%	59%	74%	42%	53%
Индекс глобальной кибербезопасности	20%	56%	59%	82%	42%	50%
Текущее исследование(ТСЫШ)	12%	18%	59%	66%	42%	56%
Разрыв						
Разрыв	42.5	25	14	15.5	15.5	3.5

Согласно таблице, наиболее сбалансированная ситуация сложилась в **Украине.** Средний процент развития ИКТ 56.5 и среднее развитие кибер-безопасности 53%. Разрыв составляет всего 3.5 процентных пункта.

Грузия является единственной страной, где развитие кибер-безопасности превышает развитие ИКТ. Средняя величина развития ИКТ составляет 58.5% и средняя величина развития кибер-безопасности- 74%. Разрыв составляет 15.5 процентных пункта и это способствует кибер-безопасности.

Следующая таблица представляет общие результаты настоящего исследования. Темно-зеленый цвет демонстрирует потенциалы, выполненные на 50% или более. Светло-зеленый цвет демонстрирует потенциалы, выполненные на 25-50%. Белый цвет демонстрирует потенциалы, выполненные менее чем на 25%.

Общий обзор результатов стран.

		Армения	Азербайджан	Беларусь	Грузия	Молдова	Украина
I	ОБЩИЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ						
1.	Разработка	0%	0%	25%	100%	38%	88%
2.	Оценка угроз	0%	75%	75%	100%	0%	0%
3.	Образование	0%	20%	55%	20%	30%	75%
4.	Международное сотрудничество	10%	30%	20%	40%	10%	20%
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ						
5.	Основная безопасность	27%	9%	55%	64%	73%	82%
6.	Безопасность э-услуг	0%	0%	100%	75%	100%	25%
7.	Э-ИД и э-подпись	25%	50%	100%	100%	100%	88%
8.	CIIP	0%	0%	100%	100%	0%	67%
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ ПРОИСШЕСТВИЯМИ И КРИЗИСОМ						
9.	CIRC	0%	44%	100%	89%	56%	67%
10.	Управление кризисом	0%	0%	11%	33%	0%	33%
11.	Киберпреступления	60%	10%	60%	100%	100%	90%
12.	Национальная защита	0%	0%	60%	20%	0%	0%

Таблица обозначает сферы, в которых у стран Европейского Партнерства хорошие показатели и области, которые нуждаются в более пристальном внимании. Мы рекомендуем установление приоритетов на областях сотрудничества, где страны Европейского Партнерства имеют общие недостатки кибер-безопасности.

Согласно результатам, мы можем сказать, что способности с наилучшим развитием являются:

- Основная безопасность
- Э-ИД и Э-подпись
- Способность реагировать на компьютерные инциденты
- Борьба с кибер-преступлениямие

Наименее развитыми областями являются:

- Развитие международной кибер-безопасности и влияния
- Управление кибер-кризисом
- Национальная обороноспособность в кибер-поле

Более специфически, обзор ситуации по кибер-безопасности стран Европейского Партнерства представлен в следующей таблице. Она дает обзор на основании ДА (x) и НЕТ (-) и показывает какие специфические способность существуют в стране и какие способности нуждаются в развитии.

Например, одна из сфер, в которых все страны Восточного Партнерства требуют развития - это знания по кибер-безопасности в начальном образовании. Существует нужда в обучении детей аспектам базовой онлайн и компьютерной безопасности. В дополнение, таблица демонстрирует, что эксперты профессиональной ассоциации по кибер/информационной безопасности существуют только в Украине. Другие страны Восточного Партнерства нуждаются в этом.

Другие сферы, в которых все страны Восточного Партнерства нуждаются в развитии - это Управление кибер-кризисом. Ни одна из стран Восточного Партнерства не имеет плана управления широкомасштабных кибер-происшествий. Центр Операций в киберпространстве существует только в Украине. Учения по управлению кибер-кризисом организованы только в Беларуси. Пара стран принимала участие в международных упражненях по управлению международным кибер-кризисом. Все эти аспекты показывают, что следует держать в фокусе развитие способность управления кибер-кризисом.

Детализированный обзор результатов стран.

		Армения	Азербайджан	Беларусь	Грузия	Молдова	Украина
I	ОБЩИЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ						
1.	Policy development	0%	0%	25%	100%	38%	88%
	Подразделение Разработки концепции	-	-	-	x	-	x
	Формат координации	-	-	x	x	-	x
	Термины и определения	-	-	-	x	x	-
	Стратегия кибербезопасности	-	-	-	x	x	x
	План внедрения	-	-	-	x	x	x

2.	Оценка угроз	0%	75%	75%	100%	0%	0%
	Подразделение оценки угроз	-	x	x	x	-	-
	Годовые публичные отчеты	-	-	-	x	-	-
3.	Образование	0%	20%	55%	20%	30%	75%
	Веб-сайт по кибербезопасности	-	x	-	x	x	x
	Увеличение общественной осведомленности	-	x	-	x	x	-
	Начальное образование	-	-	-	-	-	-
	Среднее образование	-	-	x	-	-	-
	Профессиональное образование	-	-	x	-	-	-
	Бакалавриат	-	-	x	-	x	x
	Магистратура	-	-	x	-	-	x
	Докторантура	-	-	x	-	-	x
	Профессиональная ассоциац	-	-	-	-	-	x
4.	Международное сотрудничество	10%	30%	20%	40%	10%	20%
	Подразделение взаимодействия	-	-	-	-	-	-
	Конвенция по кибербезопасности	x	x	-	x	x	x
	Соглашение о сотрудничестве	-	x	x	x	-	-
	Международное представительство	-	x	x	x	-	x
	Междунар. Орг-ции в стране	-	-	-	-	-	-
	Наращивание потенциала	-	-	-	x	-	-
II	ОСНОВНЫЕ ИНДИКАТОРЫ КИБЕРБЕЗОПАСНОСТИ						
5.	Основная безопасность	27%	9%	55%	64%	73%	82%
	Подразделение основной безопасности	-	-	x	x	-	x

	Ведомство защиты данных	x	-	-	x	x	x
	Секретная информация	-	x	x	x	x	x
	Стандарт безопасности	-	-	-	-	x	-
	Аккредитация систем ИКТ	-	-	x	-	x	x
	Аудит систем ИКТ	-	-	x	-	x	x
6.	Безопасность э-услуг	0%	0%	100%	75%	100%	25%
	Безопасность э-услуг	-	-	x	x	x	-
	Современная криптография	-	-	x	-	x	x
7.	Э-ИД и э-подпись	25%	50%	100%	100%	100%	88%
	Уникальный идентификатор	-	-	x	x	x	x
	Э-сервисы используют уникальный ИД	-	-	x	x	x	x
	2-факторная аутентификация	-	x	x	x	x	-
	Электронная подпись	x	x	x	x	x	x
	Провайдеры трастовых услуг SURYLGHUV	-	x	x	x	x	x
	Э-подпись легальна	x	x	x	x	x	x
8.	CIIP	0%	0%	100%	100%	0%	67%
	CII Ропределено	-	-	x	x	-	x
	Подразделение защиты	-	-	x	x	-	x
	Требование непрерывности	-	-	x	x	-	-
	Руководитель кибербезопасности	-	-	x	x	-	-
III	ИНДИКАТОРЫ УПРАВЛЕНИЯ ПРОИСШЕСТВИЯМИ И КРИЗИСОМ						
9.	CIRC	0%	44%	100%	89%	56%	67%
	Подразделение CIRC	-	x	x	x	x	x
	Ответственность за передачу данных	-	-	x	-	-	x

	Государственно-частное сотрудничество	-	-	x	x	-	-
	Обмен секретными данными	-	-	x	x	x	x
10.	Управление кризисом	0%	0%	11%	33%	0%	33%
	План управления кризисом	-	-	-	-	-	-
	Центр управления	-	-	-	-	-	x
	Учения с кибер комп.	-	-	-	-	-	-
	Учения по кибер-кризису	-	-	-	x	-	-
	Участие в междунар. учениях	-	-	x	x	-	-
	Использование волонтеров	-	-	-	-	-	-
11.	Киберпреступления	60%	10%	60%	100%	100%	90%
	Криминализация	x	-	x	x	x	x
	Подразделение киберпреступлений	-	-	x	x	x	x
	Подразделение цифровой криминалистики	x	-	-	x	x	x
	Доказательства регулированы	-	-	-	x	x	-
	Контактный центр 24/7	x	x	x	x	x	x
12.	Национальная защита	0%	0%	60%	20%	0%	0%
	Подразделение планирования кибер-операций	-	-	-	-	-	-
	Подразделение кибер-операций	-	-	x	-	-	-
	Учения с кибер комп.	-	-	-	x	-	-
	Учения по кибер-операциям	-	-	x	-	-	-
	Участие в междунар. учениях	-	-	x	x	-	-

Рекомендации в сфере э-демократии

Армения

- Опыт Армении в инновационном управлении (например, инновационная лаборатория Kolba Lab) следует продвигать и поощрять. Открытость и желание правительственных деятелей развивать эту сферу не могут быть переоценены.

- Армения имеет множество э-решений, у которых, однако, достаточно низкий уровень использования. Многое еще должно быть сделано в области осведомленности общественности. Необходимо поощрять все стороны к разработке всестороннего и исчерпывающего обзора инструментов э-демократии, для того, чтобы создать «меню» из различных средств, которые сможет использовать как гражданское общество, так и правительство.

- Сфера открытых данных требует более тщательного понимания со стороны всех секторов общества. Необходимо уделять внимание и развивать **способность и навыки гражданского общества** использовать потенциал технологий, а также существующие открытые данные новаторским способом. Так же, необходимо должным образом стимулировать ИТ-сообщество становится частью социальных инноваци.й

- Так как сфера открытых данных и прозрачность, которую они обеспечивают, становятся все более распространёнными направлениями, много внимания следует уделять **законодательству защиты данных**, что является вопросом, вызывающим беспокойство, согласно исследованию.

- В Армении активно развиваются инициативы на местном уровне, которые поддерживаются НКО и донорами. Важно продолжать работу в этом направлении и повышать осведомленность местных сообществ об альтернативных формах вовлечения.

- Крайне важно способствовать адаптации и приспособлению новых решений к местным нуждам. Должен быть прагматический тандем между донором и правительством, позволяющий реализовать пилотные версии новых проектов перед попыткой широкомасштабного внедрения. Вовлечение ИТ-сообщества в эти пилотные проекты (и поиск подходящего стимула для этого) может способствовать взаимодействию между неправительственным и ИТ-секторами.

Азербайджан

- Правовой и институциональный механизм и регулирование э-участия является важным. В настоящее время отсутствуют стратегии или план мероприятий для гражданского участия или э-участия. Единственный стратегический документ, который можно рассматривать как обязательство правительства относительно прозрачности и гражданского участия - это самый последний план действий в рамках инициативы Партнерство Открытого Правительства на период с 2016 по 2018 гг. Тем не менее, поскольку текущий статус Азербайджана в данной инициативе- неактивный, в настоящее время его внедрение трудно прогнозировать.

- Рекомендуется поддержка в сфере мониторинга предоставления публичной информации госсектором. Обеспечение соблюдения Закона о доступе к информации, который был утвержден в 2005 г., может находится в рамках полномочий Омбудсмена по информации, который изначально рассматривался как необходимый орган, но поздней был ликвидирован.

- Относительно предоставления информации онлайн, рекомендуется поддержка местных самоуправлений в области предоставления информации через официальные веб-страницы; например, развитие шаблона со специфическим макетом для публичной информации на веб-страницах органов местного самоуправления. Это способствовало бы более легкому доступу к информации на локальном уровне для жителей, а также обеспечение местных самоуправлений достаточно простыми инструментами для структуризации их информации.

- Акцент следует сделать на более однородное развитие э-услуг. Текущая доступность и качество э-услуг все еще неравномерные. Существуют явные лидеры среди государственных ведомств, но существуют также такие, кто отстает. Очевидно, что трансформация от предоставления услуг оффлайн до онлайн-услуг требует поддерживающего правового и институционального механизма, а также перепроектирования процессов.

- Механизм мониторинга необходим в сфере удобства использования и доступа к э-услугам, чтобы предоставить возможность гражданам использовать полный потенциал э-услуг, которые уже существуют, а также, чтобы спроектировать новые. Так же, анализ мониторинга результатов и следствий этого процесса должен быть понятным. Индекс ASAN, разработанный Агентством, также содержит вопросы мониторинга, которые покрывают такие компоненты, как э-информация и э-консультация, однако, требует более четкой ясности то, как результаты мониторинга и следствия этого процесса используются для развития э-услуг и э-участия.

Беларусь

- Существует необходимость в изменении или обновлении законодательной базы по доступу к публичной информации и защите данных, которая учитывала бы развитие в области ИКТ.

- НКО следует более интенсивно использовать новые средства массовой информации с целью продвижения своих тематик на более широкую аудиторию. Также, необходимо повышать их уровень осведомленности о концепции э-участия, чтобы способствовать комплексному развитию культуры участия в третьем секторе.

- Достаточно невысокий уровень сотрудничества между участниками третьего сектора и невысокая степень осведомленности друг о друге может представлять препятствие в достижении большего влияния. Рекомендуется увеличить количество совместных видов деятельности и вовлекать белорусское аналитическое сообщество (например, экспертов, исследователей, научно-исследовательские центры) в адвокативные кампании. Со стороны донорского сообщества, международных организаций и агентств по развитию рекомендуется инициировать совместные тематические мероприятия для обмена опытом и сотрудничества.

- Инициативы локального уровня могут стать лучшим способом для продвижения э-демократии в Беларуси. Потенциал дальнейшего развития может быть реализован через деятельность в сфере э-консультаций по значимым вопросам, например, таким, как планирование городского пространства.

Грузия

- В Грузии наблюдается преобладание инструментов э-демократии, сфокусированных на прозрачности и подотчетности. Необходимо больше инструментов э-демократии, направленных на участие граждан в процессе принятия решений. Платформа для э-петиций (ichange.gov.ge), которая сейчас примыкает к программе действий правительства, имеет потенциал, чтобы развить сферу э-демократии. С учетом относительно невысокого показателя цифровой грамотности, рекомендуется снизить порог количества подписей для петиции, чтобы не лишить граждан мотивации использовать платформу.

- Существует четкая потребность в современном отдельном акте о свободе информации. Разработка Закона о свободе информации, который затрагивает, помимо других тем, вопрос раскрытия данных публичного сектора, остается важным. Дополнительно, рекомендуется учреждение надзорного ведомства, которое следило бы за исполнением соответствующих законоположений.

- Институционализованному гражданскому обществу следует быть более активным в распространении своих идей через привлекательные каналы коммуникации. Рекомендуется более интенсивное использование социальных сетей для распространения результатов проектов хорошего управления (good governance). Повышение общественного информирования и надлежащее обучение по использованию существующих инструментов э-демократии, разработанных НКО, должны быть одними из центральных моментов в развитии этой области.

- Целевой тренинг в правительственном секторе (как на локальном, так и на национальном уровнях) по вопросу использования ИКТ для усиления демократических процессов является основополагающим. Углубление знаний государственных служащих о законодательной базе, регулирующей прозрачность принятия решений, о концепции э-участия, открытых данных и прозрачности, а также повышение информированности о различных платформах и механизмах э-консультаций и э-участия, доступных для разных стадий процесса принятия решений.

Республика Молдова

- **Механизмы координации и распределение ответственност**и между основными стейкхолдерами в области э-демократии должны быть пересмотрены, **чтобы установить понятные стратегические цели и рекомендации** для государственных учреждений в сфере предоставления услуг, а также для практик вовлечения. Область э-демократии в Молдове до сих пор была под ответственностью Центра э-правительства. Она будет перенесена в ближайшем будущем под юрисдикцию Государственной канцелярии. **Сотрудничество между Центром э-правительства и Государственной канцелярией** станет чрезвычайно важным, так же, как и инициативная работа последней в повышении общественной осведомленности о развитии э-демократии. Для того, чтобы иметь устойчивость результатов, достигнутых Центром э-правительства, этому учреждению должно быть обеспечено **стабильное финансирование** из государственного бюджета.

- Деятельность Центра э-правительства, **направленная на сбор обратной связи от граждан,** нуждается в дальнейшей поддержке и содействии. В частности, это включает такие задачи, как годовые исследования общественного мнения, которые из года в год обеспечивают ценный вклад в вопросы того, чего граждане на самом деле хотят (например, приоритизация услуг, доверие к виртуальному пространству и т.д.)

- Для улучшения **качества гражданского образования** важно установить понятный механизм сотрудничества между различными министерствами, которые координируют соответствующие сферы. Одним из важных аспектов гражданского образования является восприятие коррупции и манипуляции властью. Таким образом, важно повышать осведомленность о необходимости общественного мониторинга коррупции и о том, как она работает.

- **Э-трансформация** не может произойти быстро. Она требует хорошего **управления коммуникацией, чтобы объяснить гражданам преимущества э-правительства**, в частности, в сфере открытия данных. Также, необходимо заниматься вопросом недоверия граждан к правительству, культурным изменениям могут способствовать кампании, направленные на повышение информированности. Частью этой тематики являются так же **вопрос защиты частной информации и аспект прозрачности, которым необходимо уделять более пристальное внимание.**

- **Более сильный акцент должен быть сделан на создание спроса на доступ к открытым данным и на развитие навыков для использования этих данных**. Центр э-правительства вовлечен в проект открытых данных с донорским финансированием, который делает возможным открытие многочисленных баз данных. Тем не менее, необходимы лучшее понимание и осведомленность о том, что возможно делать с данными. Также, необходимо более активное вовлечение местных самоуправлений, поскольку много данных, которые могут потенциально быть интересны гражданам, является данными местного характера

- **Механизм сотрудничества между правительством и общественными организациями должен быть переосмыслен/улучшен**. Для этой цели был учрежден Национальный совет участия, однако, в его работе ожидаются определенные изменения. В настоящее время он не рассматривается как канал эффективной коммуникации между различными сторонами.

Украина

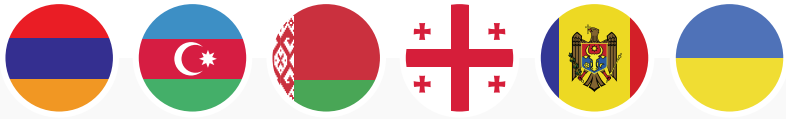
- В правительственном секторе необходима институционализация э-демократии: например, организация соответствующих департаментов и распределение человеческих и финансовых ресурсов для них. В настоящее время, Государственное агентство по э-управлению играет в этой сфере координирующую роль. Тем не менее, другие правительственные учреждения также должны быть вовлечены. Должны быть **четкие указания** для каждого учреждения, которое принимает участие во внедрении инициатив э-демократии. Коммуникационные департаменты могут быть центральными точками для деятельности и инструментов в сфере э-демократии.

- Колоссальная энергия Революции Майдана привела к институциональной и инструментальной фрагментации в области э-демократии. **Комплексный правительственный подход** в этой сфере постепенно развивается благодаря разработке Концепции э-демократии. Этому направлению и единому видению следует содействовать и способствовать его дальнейшему укреплению.

- **Активному гражданскому обществу** Украины следует продолжать выполнять активную инициативную роль в развитии э-демократии.

- Все инициативы относительно э-демократии должны сопровождаться **кампаниями и тренингами, повышающими информированность**. Хорошим примером того, как повышение осведомленности и проведение тренингов помогает построить хорошую экосистему для э-инициатив и сделать ее устойчивой, является кейс ProZorro.

- Повышение общественной осведомленности посредством **конкретных общественных проектов**, где различные стороны работают над общей программой действий, может помочь развить **культуру диалога** и, способствовать дальнейшему процветанию украинской э-демократии.



Общие рекомендации в сфере э-демократии

В виду вышесказанного, мы бы хотели очертить несколько общих рекомендаций, которые, как нам кажется, могут быть полезны для всех стран в регионе:

- Всем сторонам следует помнить о том, что ИКТ - это инструменты на службе у демократических процессов. Эти инструменты предоставляют обществу возможность улучшить и “углубить” демократию. Следовательно, не следует пренебрегать видами деятельности и мероприятиями “оффлайн”. Именно **комбинация онлайн и оффлайн средств содействует** появлению успешных практик участия.

- Всем сторонам рекомендуется сотрудничать при разработке всестороннего и исчерпывающего обзора доступных инструментов э-демократии, так называемого **“меню” из различных инструментов,** которое сможет использовать как гражданское общество, так и правительство.

- **Гражданскую активность на местном уровне следует** поощрять и поддерживать. Она играет важнейшую роль в повышении общего уровня э-активности в обществе, так как местный уровень является наиболее близким правительственным звеном к гражданам.

- **Повышение общественной осведомленности и кампании по э-грамотност**и должны быть проведены в целях борьбы с низким уровнем использования инструментов э-демократии. Также, следует разрабатывать сильные бренды инструментов э-демократии, которые ярко демонстрируют их преимущества.

- Целенаправленный тренинг **в правительственном** секторе относительно использования ИКТ для усовершенствования демократических процессов, является крайне важным. Правительствам следует рассматривать э-демократию как неотъемлемую часть э-управления и укреплять ее развитие четкими стратегическими и правовыми рамками.

Э-демократия не так сильно связана с технологиями, как с политическим и культурным выбором каждой страны относительно уровня вовлеченности граждан в политическую сферу, уровня подотчетности и открытости..