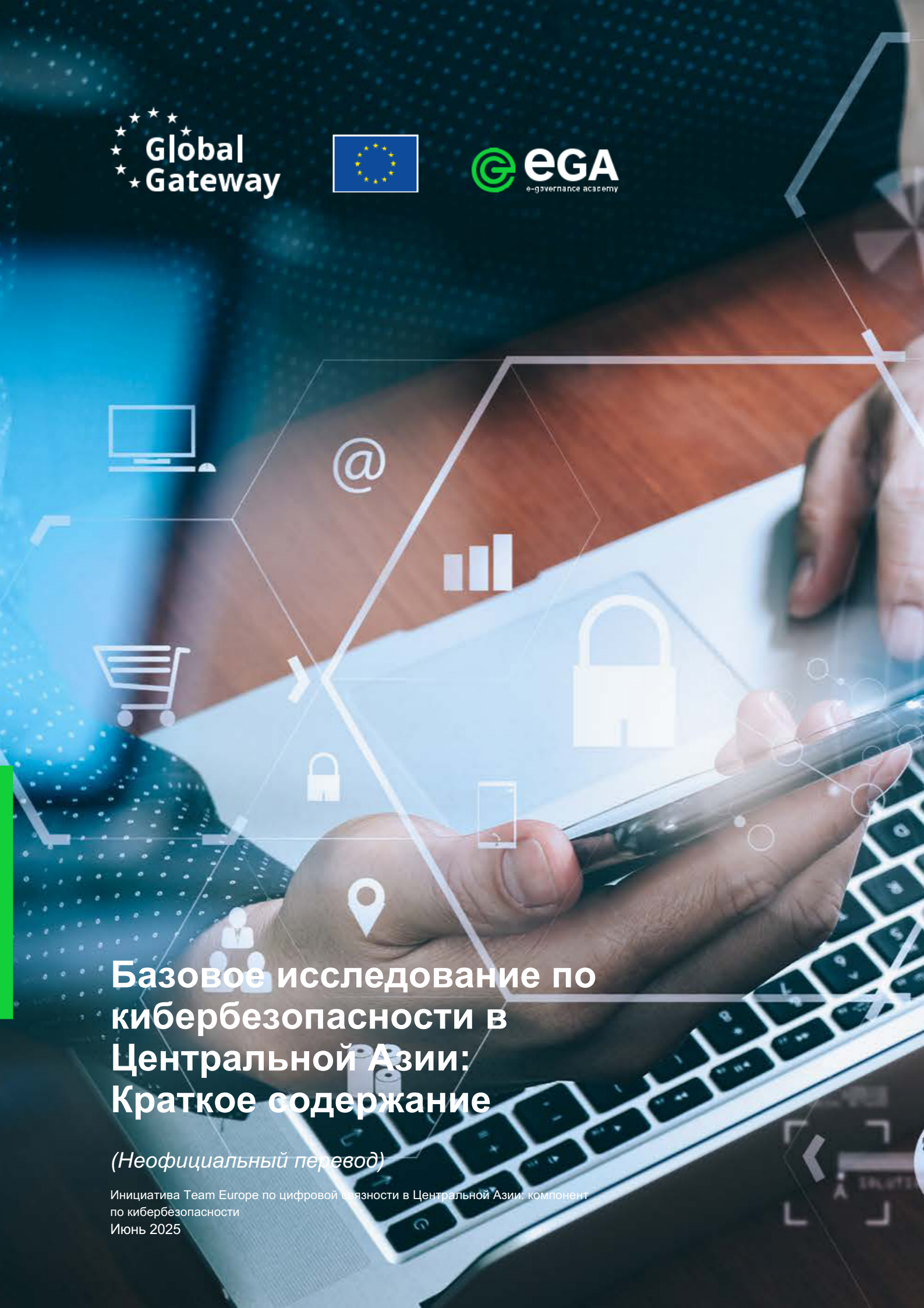


Базовое исследование по кибербезопасности в Центральной Азии: Краткое содержание

(Неофициальный перевод)

Инициатива Team Europe по цифровой связности в Центральной Азии: компонент по кибербезопасности

Июнь 2025

Авторы: Kadri Kaska, Merle Maigre, eGA (ведущие редакторы) Дизайн: Dada OÜ

Этот сводный отчет основан на национальных базовых исследованиях кибербезопасности, авторами которых являются: Siim Alatalu, Mari Tomingas-Sibul, Hanna Urva (Базовое исследование кибербезопасности Казахстана)
Markko Künnapu, Klaid Mägi, Elsa Neeme (Базовое исследование кибербезопасности Кыргызстана)
Andro Gotsiridze, Merle Maigre, Mari Tomingas-Sibul (Базовое исследование кибербезопасности Таджикистана) Piret Hirv, Mari Tomingas-Sibul (Базовое исследование кибербезопасности в Узбекистане)

Данная публикация подготовлена при поддержке Европейского Союза в рамках проекта «Инициатива Team Europe по цифровой связности в Центральной Азии: компонент по кибербезопасности» (номер контракта: Многопартнерское соглашение о сотрудничестве 700002428). Содержание данной публикации является исключительной ответственностью её авторов и никоим образом не может рассматриваться как отражающее точку зрения Европейского Союза.

Узнайте больше о проекте ega.ee/project/cybersecurity-central-asia/

Академия электронного управления (eGA) — это эстонский центр передового опыта, призванный повышать благосостояние и открытость обществ посредством цифровой трансформации. Более 20 лет мы сотрудничаем с более чем 300 организациями из 145
стран, способствуя более эффективному использованию информационно-коммуникационных технологий в государственном управлении и демократических процессах. Основу нашей команды составляют архитекторы и основатели цифрового государства Эстонии и Украины.

Узнайте больше о eGA на ega.ee

Подписывайтесь на нас в социальных сетях:

Содержание

О проекте

В этом отчете обобщены выводы компонента кибербезопасности проекта «Инициатива Команды Европы по цифровой связи в Центральной Азии». Проект направлен на содействие цифровой социально-экономической интеграции в Казахстане, Кыргызстане, Таджикистане и Узбекистане путем обеспечения безопасного и инклюзивного доступа к спутниковой связи во всем регионе.

В настоящем докладе обобщены результаты оценки, проведенной в каждой из четырех стран, и предложены действенные, не имеющие обязательной силы рекомендации для поддержки стратегического планирования, руководства взаимодействием с донорами и предоставления дорожной карты для укрепления национальной киберустойчивости.

Проект состоит из четырех компонентов:

1. Политика и нормативные акты, способствующие развитию и использованию соединительной способности ИКТ, реализуемые CPVA (ведущее), HAUS, Expertise France (EF).
2. Улучшение государственных и частных услуг по обеспечению связи, с акцентом на сельские районы, гендерное равенство и маргинализированные группы, реализуемые CFLA (ведущее), CPVA, HAUS.
3. Использование спутниковых технологий для содействия местным цифровым инновациям и решения местных проблем, реализуемое EF (lead), CFLA.
4. Фреймворки кибербезопасности, реализуемые EF и eGA.

Четвертый компонент проекта, посвященный **основам кибербезопасности**, реализуется совместно Expertise France (EF) и Академией электронного управления (eGA). Этот компонент оказывает поддержку странам-участницам в укреплении их потенциала в области кибербезопасности и повышении их способности реагировать на киберугрозы путем создания устойчивых механизмов управления кибербезопасностью и улучшения национальных возможностей в области кибербезопасности.

Эксперты eGA на встрече с заинтересованными сторонами в Таджикистане

В частности, работа включает в себя:

- Оценка национальной кибербезопасности возможностей и пробелов, а также предложение соответствующих рамок.
- Предоставление юридических, нормативных, политических и процессуальные консультационные услуги по основам кибербезопасности, соответствующие передовой международной практике.
- Обеспечение комплексного наращивания потенциала органов государственной власти, CSIRT и другие ключевые национальные заинтересованные стороны, уделяющие особое внимание технической подготовке и реагирование на инциденты.
- Повышение осведомленности общественности о проблемах кибербезопасности.
- Развитие регионального и международного сотрудничества в области кибербезопасности.

В рамках этой цели eGA провела подробное базовое исследование кибербезопасности в каждой из четырех стран-участниц, охватывающее четыре ключевые области кибербезопасности:

1. Управление, институциональные и правовые рамки,
2. Защита критической информационной инфраструктуры и управление рисками,
3. Возможности CERT/CSIRT и
4. Осведомленность общественности о цифровой безопасности.

Исследование было построено на основе трехэтапного подхода с использованием смешанных методов:

1. **Кабинетное исследование (февр–март 2025 г.),** проведенное экспертами eGA с использованием общедоступных источников и внутреннего опыта eGA. Данные были проверены с помощью широко признанных методов проверки качества информации, соответствующих тем, которые применяются при управлении Национальным индексом кибербезопасности (NCSI) eGA. На этом этапе были получены первые сведения о национальных экосистемах кибербезопасности.

2. **Опрос и полевые интервью (апр–май 2025 г.):** Полуструктурированные интервью с ключевыми национальными и международными заинтересованными сторонами, включая государственные органы, ответственные за разработку, внедрение и оценку национальных возможностей в области кибербезопасности и связанных с ними нормативных актов или законодательства, или участвующие в этой деятельности, представителей частного сектора, научных кругов и сферы образования, а также представителей делегаций Европейского союза и международных организаций, базирующихся в каждой стране.[1] Интервью проводились на основе опроса, разработанного eGA в соответствии с NCSI и моделью оценки зрелости CSIRT ENISA, и посвященного четырем основным областям кибербезопасности, указанным выше.

3. **Выезды на места (апр–май 2025)**: были посещены ключевые национальные учреждения по кибербезопасности и заинтересованные организации в каждой стране. Результаты этих встреч позволили лучше понять степень зрелости институтов и реальные проблемы..

1 Список интервью и интервьюируемых приводится в соответствующем приложении к каждому страновому отчету.

Исследование было разработано с целью предоставить подробную, всестороннюю и актуальную картину потенциала каждой страны в области кибербезопасности и ее институциональной экосистемы, что позволило бы сформировать стратегическое понимание потребностей и ресурсов, определяющих путь развития кибербезопасности в этих странах. В частности, такое понимание позволяет выявить ключевые проблемы, понять, как каждая страна может улучшить свой потенциал и институциональные рамки в области кибербезопасности, а также предложить рекомендации по развитию более высокой национальной киберустойчивости на основе проверенной на местном уровне информации и аналитических данных.

Результаты исследования отражены в отдельных базовых исследованиях по кибербезопасности для Казахстана, Кыргызстана, Таджикистана и Узбекистана. Рекомендации основаны на международных нормах и практиках, но адаптированы к местным условиям, с акцентом на региональное сотрудничество, институциональные реформы и долгосрочное наращивание потенциала. В настоящем докладе обобщены результаты оценки, проведенной в каждой из четырех стран, и представлены практические, не имеющие обязательной силы рекомендации для поддержки стратегического планирования, руководства взаимодействием с донорами и предоставления дорожной карты для укрепления национальной киберустойчивости.

Геополитический контекст и последние события

В последние годы отношения между ЕС и Центральной Азией приобрели еще большее значение, превратившись в прочное, многогранное и перспективное партнерство. Недавние изменения в политике и инициативы ЕС являются мощным преимуществом, позволяющим в рамках данного проекта предложить центральноазиатским партнерам европейские ноу-хау, опыт и модели. Участие ЕС в Центральной Азии основано на Стратегии ЕС по соединению Европы и Азии (Взаимодействие Европы и Азии: Стратегия ЕС | EEAS - Connecting Europe & Asia: The EU Strategy | EEAS) и Программе политики «Цифровое десятилетие» (Digital Decade Policy Programme 2030 | Shaping Europe's digital future), которые подчеркивают приверженность безопасной, надежной и устойчивой цифровой трансформации, в центре которой находятся люди, в соответствии с основными ценностями и фундаментальными правами ЕС.

Астана – столица Казахстана

Цифровая трансформация и кибербезопасность в регионе

На протяжении последнего десятилетия страны Центральной Азии в той или иной степени проводили экономические реформы и цифровизацию, связывая эти усилия с более широкими целями модернизации, реформы управления и геополитического позиционирования. Тем не менее, масштабы, направленность и реализация их усилий по цифровизации различаются, как и зрелость их систем кибербезопасности и возможностей.

Казахстан (KZ) географически является самой большой и богатой ресурсами страной в регионе, с населением 20 миллионов человек. Расположенный в стратегически важном месте между Китаем, Россией и республиками Центральной Азии, Казахстан находится на этапе перехода к экономике, основанной на знаниях, где цифровизация рассматривается как экономический фактор и геополитический актив. KZ стремится к быстрой цифровизации и повышению кибербезопасности за счет расширения инфраструктуры и инициатив по повышению квалификации ИТ. Новым приоритетом высокого ранга, по-видимому, стал искусственный интеллект, и в 2024 году была принята специальная стратегия.

В 2014 году KZ приняла Глобальный индекс кибербезопасности (GCI) Международного союза электросвязи (МСЭ) в качестве показателя для измерения своего прогресса в области кибербезопасности и инвестировала в разработку правовой, технической и организационной основы кибербезопасности. Она добилась значительных успехов, продемонстрировав устойчивый прогресс в индексах глобального цифрового развития и кибербезопасности. Тем не менее, в то время как цифровизация воспринимается как политический приоритет, инвестиции в кибербезопасность отстают, отражая знакомый компромисс между удобством использования и безопасностью.

Кыргызстан (KG) — парламентская республика с уровнем дохода ниже среднего и населением 7,28 миллиона человек. Страна обладает конкурентоспособным телекоммуникационным сектором, особенно в области мобильного широкополосного доступа, где уровень проникновения остаётся высоким более пяти лет, а в 2024 году началось пилотное тестирование услуг 5G. Тем не менее, в целом внедрение технологий не демонстрирует значительного прогресса, а международные индексы указывают на существенные пробелы в нормативно-правовой среде ИКТ и качестве регулирования. Кибербезопасность получила большее внимание в политической повестке в ответ на рост уровня угроз, однако страна всё ещё находится на начальном этапе зрелости в этой сфере — фиксируется базовая приверженность принципам кибербезопасности, но сохраняются недостатки в институциональных возможностях и межведомственном сотрудничестве.

Таджикистан (TJ), С населением около 10 миллионов человек, он по-прежнему находится на ранних стадиях цифровой трансформации и испытывает недостаточные инвестиции в цифровое управление и кибербезопасность. Ее цифровая инфраструктура недостаточно развита, и, признавая важность цифровизации, стране не хватает последовательной национальной стратегии или институциональной основы для ее поддержки. Последние международные индексы

подчеркивают необходимость правовой и политической реформы, при этом низкие показатели по стратегическим, организационным и техническим возможностям. Наметились признаки прогресса в основных правовых положениях (киберпреступность).

Узбекистан (UZ), с населением 35 миллионов человек, является экономическим регионом с доходом ниже среднего и граничит со всеми другими республиками Центральной Азии. Обладая богатыми природными ресурсами и традиционным промышленным производством, в последние годы она проводит обширные экономические и социальные реформы и активно работает над привлечением иностранных инвестиций. Правительственные программы модернизировали и расширили цифровую инфраструктуру. Страна также повышает скорость интернета и объем услуг ИКТ. Рынок мобильного широкополосного доступа находится в стадии быстрого роста, что обусловлено высоким спросом на цифровые услуги со стороны молодого населения. В связи с быстрым ростом рыночного спроса на цифровые услуги и объемов услуг, а также растущей проблемой киберпреступности, правительство все чаще уделяет приоритетное внимание кибербезопасности. В 2024 году МСЭ отнес Узбекистан к *категории Tier 2* – Продвинутая категория, которая обозначает значительный прогресс в развитии кибербезопасности. Его относительными сильными сторонами являются сотрудничество, правовые меры и меры по развитию потенциала, в то время как техническая и организационная зрелость все еще развивается.

Цифровизация	Индекс развития ИКТ 2024	90.1	88.3	N/A	81.7
	Индекс готовности сетей 2024	50.52 (61st)	44.16 (86th)	N/A	44.87 (81st)
	Индекс ООН развития э-правительства 2024	0.9009 (24th)	0.7316 (78th)	0.5606 (123rd)	0.7999 (63rd)
Кибербезопасность	Национальный индекс кибербезопасности (NCSI)	70.83 (32nd)	60.00 (40th)	15.83 (84th)	55.00 (50th)
	Глобальный индексl кибербезопасности МСЭ (2024)	Уровень 2 – Передовой (94.4)	Уровень 3 – Установление (65.59)	Уровень 4 – Развивающийся (25.36)	Уровень 2 – Передовой (89.2)

Среда киберугроз и тенденции

Кибератаки в последние годы стали более разнообразными и масштабными во всех четырёх странах. Наиболее частыми целями становятся финансовые учреждения, государственные органы и средства массовой информации. Также фиксируются атаки на промышленность и критическую инфраструктуру, а отдельные кампании направлены против журналистов и политических активистов, преимущественно в Кыргызстане.
Наиболее распространённые векторы угроз включают вредоносное программное обеспечение (особенно программы-вымогатели), фишинг и кражу учётных данных, а также эксплуатацию публичных информационных систем, что приводит к утечкам данных и компрометации систем с последующим нарушением их работы. Также зафиксированы случаи захвата электронных почтовых и аккаунтов в соцсетях, публикации личной информации (doxxing), а также распространения вредоносного ПО на мобильных устройствах — особенно в Казахстане.

Низкий уровень осведомлённости о кибербезопасности, широкое использование устаревшего или нелицензионного программного обеспечения, а также заражённых внешних устройств — всё это, что является распространённым явлением по всему региону, — усугубляет уязвимости. Несмотря на то что частный сектор, особенно в сфере финансов и телекоммуникаций, усилил меры кибербезопасности, инфраструктура государственного сектора остаётся уязвимой.

Недостаточная осведомленность о кибербезопасности, широкое использование устаревшего или нелицензионного программного обеспечения и зараженные внешние устройства – все это распространено по всему региону – усугубляют уязвимости.

В Таджикистане многие правительственные веб-сайты не имеют сертификатов безопасности, а широкое использование государственных учреждениями иностранных серверов и облачных почтовых сервисов вызывает обеспокоенность в отношении суверенитета данных и юрисдикции.

Примечательно, что в регионе активно действуют изощренные злоумышленники. В 2025 году группа, получившая название «Безмолвная рысь», нацелилась на Кыргызстан и соседние государства, используя сложные многоступенчатые атаки, направленные на правительственные и дипломатические учреждения. Они использовали социальную инженерию и извлекали данные через ботов Telegram. С 2020 года Таджикистан находится в центре длительного кибершпионажа со стороны связанной с Россией группировки Nomadic Octopus (DustSquad), которая проникла в телекоммуникационную инфраструктуру для слежки за высокопоставленными правительственными чиновниками и государственными системами. Несмотря на то, что их инструменты не были технически сложными, им удалось скомпрометировать широкий спектр сетей и устройств.

Улицы в Самарканде, Узбекистан

Выводы

Эксперты eGA на встрече с заинтересованными сторонами в Казахстане

Стратегическая и правовая основа для кибербезопасности

Четыре страны Центральной Азии стремятся интегрировать кибербезопасность в свои более широкие цифровые повестки дня, но подходы значительно различаются по приоритетам, зрелости и реализации. Эффективное управление и устойчивость во всем регионе подрываются сохраняющимися пробелами в правовой базе, институциональной ясности и правоприменительном потенциале.

Казахстан лидирует с наиболее прочной стратегической основой, основанной на его стратегиях «Киберщит» (2017, 2022 годы) и Концепции цифровой трансформации, развития ИКТ и кибербезопасности 2023 года. **Кыргызстан** и **Узбекистан** встраивают кибербезопасность в стратегии цифровизации, однако обе страны все еще обновляют правовую базу и институциональные структуры. **Таджикистан** находится на более зачаточном этапе разработки политики, разрабатывая свою первую национальную стратегию кибербезопасности при поддержке МСЭ. Три страны (Казахстан, Таджикистан и Узбекистан) также заявили о своих амбициях в отношении искусственного интеллекта, приняв специальные стратегии.

Стратегическая повестка в области кибербезопасности в регионе обычно нацелены на инфраструктурное и институциональное развитие, возможности реагирования на инциденты, защиту персональных данных информирование общественности и правовую реформу. Тем не менее, существуют следующие проблемы при реализации:

- пересекающиеся полномочия государственных учреждений,
- непоследовательное применение концепций и терминологии,
- ограниченное планирование на случай непредвиденных обстоятельств, и
- нехватка квалифицированных кадров является обычным явлением.

В Узбекистане институциональные обязанности еще четко не определены, и механизмы координации могут быть еще больше укреплены. Новый закон Кыргызстана о кибербезопасности ожидает принятия нескольких актов, в то же время являясь частью продолжающегося более широкого пересмотра цифрового управления. Таджикистан сталкивается с ограничениями во взаимодействии с заинтересованными сторонами и имеет возможности для повышения инклюзивности своих политических процессов.

Эффективному управлению и устойчивости во всем регионе препятствуют сохраняющиеся пробелы в нормативно-правовой базе, институциональной ясности и в правоприменительном потенциале.

Во всем регионе к кибербезопасности часто подходят через призму защиты персональных данных, что сужает институциональные полномочия и проблемы в соответствии с более широкими целями национальной безопасности, критически важной устойчивости инфраструктуры и непрерывности цифровых услуг.

Юридические ссылки на кибербезопасность разбросаны по законам о защите данных, телекоммуникациях, электронной коммерции и электронных подписях, их применение часто слабое, а подотчетность регулирующих органов остается ограниченной. В частности, Таджикистан сталкивается с проблемами, связанными с дублированием и пробелами в институциональной системе, при этом ответственность не всегда четко определена, а полномочия регулирующих органов остаются в значительной степени ограниченными на практике. Более четкие мандаты, координация между государственными учреждениями и практические механизмы обеспечения соблюдения остаются важными областями для развития во всех четырех странах.

С точки зрения законодательства о кибербезопасности, Казахстан и Кыргызстан предусматривают обозначение КИИ и связанные с этим обязательства в национальном законодательстве; В Казахстане также введен обязательный мониторинг инцидентов, связанных с аудитом ИКТ. В Узбекистане действуют официальные полномочия CERT и правила сертификации, но практическое применение ограничено, и некоторые оперативные системы устойчивости CII могут быть улучшены. Система реагирования Кыргызстана все еще находится в стадии разработки, и в Таджикистане до сих пор не создана функционирующая КИИ или полностью применимые структуры реагирования на инциденты.

Все страны все больше осознают международные рамки, такие как GDPR ЕС или Будапештская конвенция Совета Европы, и в той или иной степени заинтересованы в гармонизации, но цели различаются. Казахстан, например, заинтересован в извлечении полезных элементов, а не в полном согласовании, в том числе для разработки нового закона об искусственном интеллекте. Она с осторожностью относится к чрезмерному регулированию, которое рассматривается как проблематичное в ЕС из-за его потенциала ограничивать или сдерживать инновации.

Основные учреждения, ответственные за кибербезопасность

В большинстве стран Центральной Азии в настоящее время назначены ведущие министерства или национальные агентства, которым поручено разрабатывать и координировать политику в области кибербезопасности, как правило, в министерствах цифрового развития или инноваций. Тем не менее, сохраняются общие институциональные проблемы, связанные с некоторыми дублирующими мандатами (в частности, в Узбекистане и Таджикистане), отсутствием четких механизмов межведомственной координации и слабым правоприменительным потенциалом. Все страны также сообщают о нехватке квалифицированных кадров.

Казахстан имеет наиболее зрелую институциональную структуру с двухуровневой структурой управления (Комитет информационной безопасности при Министерстве цифрового развития, инноваций и аэрокосмической промышленности и Государственная техническая служба при Комитете национальной безопасности) с определенными ролями в политике, регулировании и техническом надзоре. Он также

Эксперты eGA на встрече с заинтересованными сторонами в Кыргызстане

Сохраняются общие институциональные проблемы, связанные с дублированием мандатов, отсутствием четких механизмов межведомственной координации и слабым правоприменительным потенциалом.
Все страны также сообщают о нехватке квалифицированных кадров.

выделяется благодаря созданной инфраструктуре CERT и SOC. **Система** управления кибербезопасностью в Кыргызстане также демонстрирует относительно хорошо развитую структуру, поскольку она развивается и совершенствуется. Министерство цифрового развития и инновационных технологий, в числе задач, связанных с цифровизацией, отвечает за политику в области кибербезопасности, а Координационный центр при Комитете государственной безопасности является основным государственным органом, ответственным за реализацию политики и управление национальной CERT. Недавние институциональные разработки (такие как новый SOC) указывают на дальнейший прогресс, но ключевые имплементационные акты все еще не приняты.

Таджикистан находится на ранних стадиях развития, с четкими обязательствами на уровне правительства по укреплению национального потенциала в области кибербезопасности. Создается институциональная база с новыми органами, такими как Служба коммуникаций при Правительстве и Агентство инноваций и цифровых технологий, созданное в 2024 году, которому поручено как стратегическое, так и оперативное лидерство в области кибербезопасности и которые выступают в качестве основного драйвера цифровой трансформации и соответствующего законодательства в стране.

Узбекистан формализовал свою институциональную архитектуру, в том числе Центр кибербезопасности при Службе государственной безопасности, но законодательство остается фрагментарным и не имеет ясности в отношении институциональных полномочий. Компетенция UZ-CERT узко ориентирована на государственные системы. Такие организации, как Узкомназорат, оказывают поддержку в области регулирования, но межведомственное сотрудничество и межсекторальное взаимодействие слабы.

Также растет признание важности государственно-частного партнерства, особенно в Казахстане и Кыргызстане. Казахстан наладил конструктивное взаимодействие между государственным и частным секторами (например, с TSARKA, ведущим частным CERT, и Transtelekom, крупным оператором связи с собственным CERT) с крупнейшими ИКТ оператором

АО «Национальные информационные технологии» (НИТЭК), управляющий инфраструктурой электронного правительства Казахстана, работающий в режиме 24/7 SOC, а также взаимодействующий как с частными, так и с государственными организациями на международном уровне. В Кыргызстане развивается, хотя и ограниченная, координация с частным сектором. Такие инициативы Таджикистана, как IT-парк и планируемый центр обработки данных уровня 3 в рамках «Умного города Душанбе», указывают на национальные амбиции, в то время как их успех зависит от устойчивых ресурсов и постоянного развития навыков. Создание Университета инноваций и цифровых технологий указывает на приверженность правительства Таджикистана наращиванию долгосрочных цифровых компетенций.

Встреча экспертов eGA с заинтересованными сторонами в Казахстане

Международное сотрудничество и наращивание потенциала

Центральная Азия движется к большей международной интеграции в области кибербезопасности, при этом все четыре страны участвуют в международном сотрудничестве, хотя и с различными стратегиями, специфичными для каждой страны. В то время как взаимодействие расширяется с помощью договоров, многосторонних платформ и двусторонних партнерств, оперативный потенциал должен догонять стратегические амбиции, и есть возможности для повышения институциональной преемственности. Кибердипломатия в целом остается второстепенной задачей в рамках более широких министерств (напр, по торговле или безопасности)

Regional cooperation is increasing, with several cross-border cybercrime projects and joint training exercises by OSCE.

по всему региону. Тем не менее, существует очевидный интерес и способность воспринимать международную поддержку, особенно со стороны ЕС и других ключевых партнеров.

Казахстан лидирует как в дипломатическом, так и в оперативном взаимодействии, стремясь позиционировать себя в качестве регионального лидера в области цифровизации и кибербезопасности. Его официальные лица подчеркивают автономию в навигации между западными, российскими и китайскими моделями. Казахстан активно участвует в работе ООН (РГОС), ОБСЕ (рабочая группа по безопасности ИКТ, Меры доверия) и в 2023 году был приглашен присоединиться к Будапештской конвенции. Она является участником структур ОДКБ, СНГ, ШОС и OTS и принимала у себя региональные мероприятия по кибербезопасности. Ее национальные и частные сертификаты (KZ-CERT, TSARKA) подключены к международным платформам, таким как OIC-CERT и CAMP. Государственная техническая служба (ГНС) подписала меморандумы о взаимопонимании по кибербезопасности с Турцией, Азербайджаном и Афганистаном.

Кыргызстан делает упор на согласование стандартов и техническое сотрудничество, работая над гармонизацией своих стандартов кибербезопасности с международными стандартами, такими как ISO/IEC, IEEE и IETF, а также с российским ГОСТом. Несмотря на то, что его институциональная база все еще развивается, он извлекает выгоду из постоянного участия доноров и инвестирует в международные партнерства по наращиванию потенциала, в частности, с ОБСЕ, KOICA и ЕС.

Узбекистан придерживается политики неприсоединения, но выступает за большую связь внутри и за пределами Центральной Азии. Оставаясь вне ОДКБ и участвуя в рамках СНГ и ШОС она является скромной, она участвует в сетях МСЭ, ОБСЕ, ОИС и САМР. Она также участвует в двусторонних и региональных меморандумах о взаимопонимании, в том числе с Туркменистаном. Сотрудничество с ЕС и Соединенными Штатами продолжает развиваться, особенно в области киберустойчивости и цифрового управления.

Таджикистан остается на ранней стадии развития, но наращивает компетенции с помощью программ, финансируемых донорами. Новое Агентство по инновациям и цифровым технологиям является центральным координационным органом по цифровому сотрудничеству, в настоящее время участвующим в проектах, финансируемых из внешних источников, на сумму более 170 миллионов евро. Тем не менее, она сталкивается с проблемами институциональной преемственности и способности к освоению.

Все четыре страны извлекают выгоду из усилий по наращиванию потенциала с разным уровнем глубины и координации. Казахстан и Кыргызстан участвуют в региональных учениях ОБСЕ; Кыргызстан также участвует в проектах ЕС Twinning и KOICA SOC. Узбекистан пользуется двусторонней поддержкой ЕС и США, в то время как Таджикистан в значительной степени полагается на платформы координации доноров, такие как Рабочая группа по цифровому развитию.

Regional cooperation is increasing, with several cross-border cybercrime projects and joint training exercises by OSCE. However, donor-driven efforts often lack long-term sustainability, making handover strategies, domestic training budgets, and clearer institutional anchoring essential. International support can add most value where it reinforces country-led reforms and strengthens long-term institutional capacity. Where appropriate, efforts to fos-ter regional and donor coordination could reduce duplication, align investments, and reduce strain on the existing limited capac-ities in target countries to improve their impact and effectiveness.

Защита критической информационной инфраструктуры и управление рисками

Все четыре страны признают исключительную важность защиты критической информационной инфраструктуры (КИИ), но находятся на разных уровнях правовой и операционной зрелости. Правовая база существует, но ее реализация неравномерна, и остаются заметные пробелы в идентификации КИИ и управлении рисками, институциональных мандатах и технических возможностях.

Kazakhstan has the most advanced framework. A 2022 governmental decree formalised the status of ‘critically signifi-cant objects of information and commu-nication infrastructure’ and mandated stringent cybersecurity requirements, which include SOC-style operational infor-mation security centres (OTsIB), incident monitoring, reporting, and audit obligations, as well as service location and reliability requirements. In 2023, 514 objects were classified as critical. Механизм ежегодного обзора,

К числу общих региональных проблем относятся неясные институциональные мандаты, дублирование регулирующих функций и неравномерность технических возможностей государственных и частных операторов.

Курируется Министерством цифрового развития, инноваций и аэрокосмической промышленности, поддерживает классификацию в актуальном состоянии. Тем не менее, стандарты безопасности различаются, как и организационные различия с точки зрения реализации. Существует только 54 сертифицированных OTsIB, и жесткий процесс лицензирования соответствует контролю качества, поскольку отсутствует механизм повторной оценки или отзыва.

С апреля 2025 года в **Кыргызстане** вступили в силу основные нормативные акты по внедрению, определяющие секторы КИИ, критерии идентификации КИИ и систему сертификации инструментов кибербезопасности, а также требования к аудиту кибербезопасности. Тем не менее, необходимая методология идентификации КИИ все еще находится на рассмотрении, и закон еще не реализован на практике. Требования к информационной безопасности, предназначенные для применения государственными структурами и операторами КИИ, находятся только на ранних стадиях разработки.

Таджикистан находится на начальном этапе развития. В настоящее время его законодательство распространяется только на государственные учреждения, и не существует обозначения или реестра КИИ. В настоящее время разрабатывается национальная стратегия кибербезопасности (2025–2030 годы), а процессы взаимодействия с частным сектором и управления рисками только формируются. Практическая реализация потребует существенного наращивания потенциала и межведомственной координации.

В Узбекистане в соответствии с Законом о кибербезопасности 2022 года предусмотрены широкие определения КИИ и классификация на основе рисков. Он предусматривает системы мониторинга, отчетности и смягчения последствий, но их реализация остается непоследовательной. Многие операторы не уверены в своем статусе или обязательствах, а реализация требований кибербезопасности сталкивается с многочисленными институциональными и техническими проблемами. Центральный банк Узбекистана CERT (CERT-CBU) в банковском секторе является редким примером более продвинутой зрелости в конкретном секторе.

К числу общих региональных проблем относятся неясные институциональные полномочия, дублирование регулирующих функций (например, операторы связи также выступают в качестве регулирующих органов в Таджикистане и Узбекистане) и неравномерность технического потенциала государственных и частных операторов. Механизмы реагирования на инциденты доступны в основном там, где законодательная зрелость выше (KZ, UZ), но даже в этом случае большинству стран еще предстоит создать комплексное планирование реагирования на кризисы и регулярное тестирование.

Отраслевой уровень готовности сильнее в банковском деле и энергетике, чем в здравоохранении, образовании или общем управлении. Растущая потребность в политиках использования облака и стандартах информационной безопасности локальных центров обработки данных, по-видимому, усложняет работу, поскольку полный запрет на использование облака является серьезным препятствием для модернизации цифровых сервисов и обеспечения устойчивости.

Kazakhstan has adopted a national cyber crisis response plan, but it needs to be tested through cybersecurity exercises. Uzbekistan has expressed strong interest in tabletop exercises and train-the-trainer formats to test joint incident response readiness and support the creation of a national cyber incident master plan.

Несмотря на то, что основополагающие элементы в той или иной степени уже созданы, Кыргызстан и Таджикистан выиграют от дальнейшей поддержки в создании реестров CII, систем управления рисками и функциональных систем управления. Во всем регионе существует потребность в улучшении координации между заинтересованными сторонами из государственного и частного секторов, оценке рисков в конкретных секторах, а также в целенаправленном обучении и сертификации для создания устойчивой рабочей силы в области кибербезопасности.

Потенциал команд CERT/CSIRT

Все страны, участвующие в исследовании, признают важность CERTs/CSIRT и стремятся создать или расширить возможности реагирования на инциденты. Казахстан лидирует благодаря зрелой, многоуровневой экосистеме CERT, объединяющей публичные и частные CERT (все они являются членами FIRST), которые предлагают расширенные услуги, такие как обнаружение вторжений, анализ вредоносного ПО, оценка уязвимостей.

и так далее. Защиту критической инфраструктуры поддерживают более 50 центров технического реагирования (ЦБИ), которые в настоящее время охватывают около 10% операторов КИИ и их число увеличивается в связи с требованиями законодательства. Тесное сотрудничество между государственным и частным секторами, в частности между СТС и ЦАРКА, укрепляет оперативную мощь Казахстана.

В Кыргызстане есть частично функционирующая национальная CERT, но она по-прежнему испытывает нехватку ресурсов и пробелы в технической экспертизе. В Узбекистане действуют две CERT (одна на базе правительства, другая при Центральном банке), ориентированные на государственные услуги и финансовый сектор. Таджикистан все еще находится на стадии планирования, и его национальная CERT еще не создана.

Однако за пределами Казахстана дублирование институциональных мандатов, постепенное улучшение межсекторальной координации и неясная роль частного сектора продолжают создавать проблемы. Существует общий интерес к присоединению к глобальным и региональным платформам кибербезопасности, таким как FIRST и OIC-CERT, а также к разработке отраслевых CERT, в частности, для финансов. Кроме того, нехватка рабочей силы характерна для всего региона, что связано с нехваткой знаний в области анализа вредоносного ПО, поиска угроз и реагирования на инциденты. Квалифицированные специалисты по кибербезопасности, как правило, сосредоточены в столицах, при этом возможности для обучения специалистов ограничены.

Несмотря на то, что стратегическое направление четко определено, а международное согласование является приоритетом, необходима дальнейшая поддержка для укрепления координации, развития специализированного опыта и расширения потенциала реагирования за пределы городских центров.

Казахстан лидирует благодаря зрелой, многоуровневой экосистеме CERT, объединяющей публичные и частные CERT.

	Казахстан	Кыргызстан	Тажикистан	Узбекистан
Статус национального CERT	Полностью действующий	Частично действующий	Не создан	Действует в рамках национальной безопасности
Секторальные CSIRT (группа реагирования на инциденты, связанные с компьютерной безопасностью**)**	Финансовый+ обязательный		Планирование ведется в рамках проекта стратегии	Финансовый (Национальный банк)
Роль частного сектора	Активное участие (TSARKA и др.)	Отсутствует	Минимальная, ситуативный ответ	С помощью CERT Национального банка
Международное сотрудничество	Члены FIRST (*Форум групп реагирования на происшествия и обеспечения безопасности*), обмен информацией об угрозах	Член OIC CERT, планы для FIRST	Поддержка МСЭ и ЕС в настройке	Часть FIRST/OIC CERT, только финансое

Обучение кибербезопасности

Эти четыре страны находятся на противоположных концах шкалы в интеграции обучения кибербезопасности в систему государственного образования. **Казахстан** и Кыргызстан внедрили цифровую грамотность и кибербезопасность в официальные школьные программы. Казахстан сотрудничает с международными структурами, такими как ЮНИСЕФ, и предлагает внеклассное обучение в рамках таких инициатив, как Кибершкола TSARKA. **Кыргызстан** также внедрил базовый контент о цифровой безопасности в образовательную политику. В отличие от этого, **Таджикистан** и Узбекистан сталкиваются с проблемой нестабильного подключения к Интернету за пределами крупных городов, а также нехватки квалифицированных учителей в области ИКТ. Тем не менее, обе страны предпринимают шаги, чтобы наверстать упущенное: Министерство образования Таджикистана проводит подготовку учителей и внедряет в школах темы кибергигиены, а Узбекистан адаптировал Руководящие указания МСЭ по безопасности в Интернете для использования на национальном уровне.

Высшее образование в области кибербезопасности расширяется. В Казахстане, Кыргызстане и Узбекистане существуют специальные программы бакалавриата и магистратуры, а в Таджикистане базовые программы по кибербезопасности встраиваются в более широкие программы в области ИКТ. Университеты начали приводить учебные программы в соответствие с международными рекомендациями и теперь включают такие темы, как сетевая безопасность, криптография и, все чаще, цифровая криминалистика и киберправо, а в некоторых государственных учебных заведениях были запущены программы по киберпреступности и киберправу.

Казахстан поддерживает доступ к высшему образованию с помощью стипендиальных программ и поощряет отраслевые партнерства и программы практического обучения, такие как соревнования Capture the Flag (CTF), которые привносят практическую подготовку в традиционно теоретическое высшее образование. Инициативы по обучению под руководством частного сектора в Казахстане и Кыргызстане также предлагают практическое, основанное на навыках обучение как для государственных органов, так и для специалистов отрасли.

Исследования в области кибербезопасности ограничены, но растут, и в Кыргызстане есть специализированный центр, специализирующийся на прикладных исследованиях. Межуниверситетское сотрудничество остается недостаточно развитым, хотя партнерские отношения с международными и частными субъектами расширяются (причем последние, как правило, возглавляются частным сектором, а не научными кругами).

Однако, несмотря на достигнутый прогресс, сохраняются пробелы в подготовке кадров в государственном секторе, исследовательской инфраструктуре и межсекторальной координации.

В целом, несмотря на отсутствие единой модели в регионе, траектория движения идет в сторону большей институционализации, практического взаимодействия и сотрудничества заинтересованных сторон. Международная поддержка, в частности со стороны МСЭ и ОБСЕ, способствовала наращиванию потенциала с помощью целевых программ, ориентированных в основном на государственный (например, правоохранительные органы) и технический персонал (судебно-медицинская экспертиза). Однако, несмотря на достигнутый прогресс, сохраняются пробелы в подготовке кадров в государственном секторе, исследовательской инфраструктуре и межсекторальной координации.

Осведомленность общественности в области кибербезопасности

Общая осведомленность общественности о кибербезопасности остается низкой, особенно среди пожилых людей и сельского населения. Несмотря на то, что мобильные устройства широко используются, знания о киберрисках и индивидуальной защите данных ограничены, и многие граждане по-прежнему ожидают, что государство защитит от них киберугрозы, а не понимают индивидуальную ответственность и свободу действий. Осведомленность среди женщин и пожилых людей особенно низка.

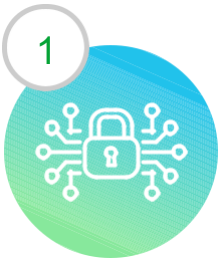
Казахстан выделяется рядом информационных кампаний, проведенных в последние годы как государственными органами, так и представителями гражданского общества; он предоставляет платформу онлайн-обучения (аналогичная инициатива существует в **Узбекистане**) и ежегодный тренинг по кибергигиене для государственных служащих. **В Агентстве по** защите персональных данных Кыргызстана есть специальный учебный центр, и **Таджикистан** полагается на менее масштабные усилия под руководством групп гражданского общества, хотя и с ограниченным охватом и финансированием.

Усилия по повышению осведомленности часто носят фрагментарный характер и основаны на проектах, при этом их эффективность не согласуется и не координируется между субъектами. Несмотря на растущее признание потребности в цифровой грамотности и грамотности в области кибербезопасности, скоординированные и устойчиво финансируемые национальные стратегии нуждаются в дальнейшем совершенствовании.

Общая осведомленность общественности о кибербезопасности остается низкой, особенно среди пожилых людей и сельского населения.

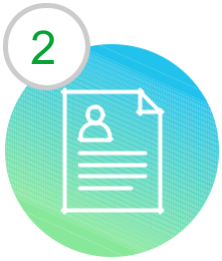
Восемь рекомендаций

Основываясь на этих выводах, в исследовании рассматриваются целевые действия, организованные по тематическим областям, с акцентом на действия, которые должны быть предприняты национальными заинтересованными сторонами, и поддержку, которую может предложить проект.



Разработка стратегий кибербезопасности

Для укрепления стратегического планирования кибербезопасности в исследовании рекомендуется адресная поддержка разработки и уточнения национальных стратегий кибербезопасности и связанных с ними программных документов, согласования стратегии кибербезопасности с цифровой трансформацией и включения принципов корпоративного управления, управления рисками и комплаенса в национальный стратегический инструментарий. Помощь может включать в себя сравнительные выводы государств-членов ЕС, технические рекомендации по структурированию стратегических рамок, вклад в работу национальных рабочих групп и экспертный вклад в разработку политики. Тестируемые модели следует продвигать, чтобы гарантировать, что стратегии последовательны, реалистичны и оказывают влияние. В ходе этих мероприятий следует уделять внимание согласованию национальных целей с международными стандартами и передовой практикой, в том числе отраженными в подходе ЕС к кибербезопасности.



Developing legal frameworks

В целях поддержки разработки современных и согласованных правовых рамок исследование рекомендует предоставить помощь ЕС в подготовке и пересмотре законодательства, связанного с кибербезопасностью, используя в качестве ориентиров директиву NIS2, Общий регламент по защите данных (GDPR), Акт об ИИ и eIDAS (директива о электронной идентификации, аутентификации и доверительных услугах. Приоритетными областями для законодательных действий являются требования к информационной безопасности государственного сектора, обязанности поставщиков CII и задачи, связанные с предотвращением инцидентов и реагированием на них, с акцентом на модернизацию терминологии, уточнение институциональных ролей и согласование механизмов реализации. Поддержка проекта должна выходить за рамки первичного законодательства и включать в себя внедрение нормативных актов, методологий и процедур. Кроме того, учитывая, что национальные заинтересованные стороны подчеркнули необходимость практического руководства, такие инструменты, как шаблоны моделей, семинары под руководством экспертов, консультативная поддержка и обмен передовым опытом ЕС по реализации, могут быть полезными. Кроме того, в рамках данной работы следует учитывать такие мероприятия, как взаимодействие с заинтересованными сторонами и обеспечение последовательности в толковании и применении, такие виды деятельности, как обмен мнениями по правовым вопросам, целевое обучение и консультации с заинтересованными сторонами.

Укрепление интституционального потенциала

Для укрепления институционального потенциала целевая поддержка должна быть направлена на повышение квалификации юридического, политического и операционного персонала через структурированные программы обучения, технические семинары и поддержку учебных курсов, соответствующих международным нормам в области кибербезопасности. Участие в международных конференциях, учебных визитах и региональных диалогах поощряется в целях содействия трансграничному сотрудничеству и обмену знаниями.

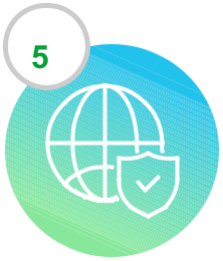
Особое внимание следует также уделять уточнению межведомственных ролей и обеспечению более структурированной координации между органами государственного сектора и заинтересованными сторонами из частного сектора. Уточнение национальной роли и полномочий должно распространяться на специализированные отраслевые учреждения для формализации их роли в институциональной архитектуре. Должны быть созданы официальные платформы для сотрудничества между государственным и частным секторами, охватывающие области разработки политики, планирования рисков и реагирования на инциденты. Поддержка проекта в этой области может основываться на моделях ЕС для обеспечения структурированного, подотчетного сотрудничества с частным сектором и субъектами гражданского общества; там, где это уместно, могут быть выявлены успешные внутренние инициативы и расширены за счет целевой технической помощи и участия в региональных сетях или сетях, поддерживаемых ЕС. Кроме того, формализация стратегического сотрудничества с надежными европейскими партнерами обеспечит устойчивую передачу знаний и приведение их в соответствие с передовым международным опытом.

Укрепление критической информационной инфраструктуры

Для повышений устойчивости критической информационной инфраструктуры, в исследовании рекомендуется целенаправленная поддержка разработки правовых и процессуальных рамок для определения CII с четкими критериями назначения, а также принятия стандартов безопасности, систем управления рисками и механизмов надзора за соблюдением требований. Помощь проекту может включать обмен опытом ЕС в области методологии идентификации и классификации критической инфраструктуры, методологии управления рисками и руководства по надзорным и аудиторским системам. Приоритетное внимание следует уделять техническому обучению по стандартам управления рисками и информационной безопасности, дополняя его обменом передовым опытом.

Особого внимания требует потенциал отраслевых регуляторов и операторов КИИ: следует содействовать повышению готовности за счет повышения квалификации в области реагирования на инциденты, разведки угроз и безопасности ICS/SCADA, уделяя особое внимание форматам обучения по конкретным специальностям и подготовки инструкторов. Технические и командно-штабные учения при поддержке национальных киберполигонов должны проводиться на институциональном и межведомственном уровнях для отработки мер реагирования на кризисы и содействия региональному сотрудничеству. Как отмечалось выше, государственно-частные платформы для обмена информацией об угрозах и планирования рисков необходимы для укрепления доверия и обеспечения скоординированных действий. Следует и далее поощрять страны к институционализации планов реагирования на инциденты и их проверке в рамках национальных и региональных учений.

Поддержка также может быть направлена на оценку рисков кибербезопасности в новых технологиях, включая биометрическую цифровую идентификацию и услуги с поддержкой искусственного интеллекта, а также помочь в разработке стандартов сертификации в соответствии с практикой ЕС.

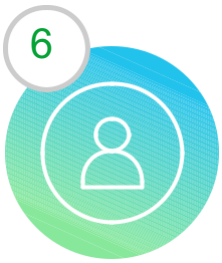


Укрепление потенциала CERT/CSIRT

Для укрепления национальных возможностей CERT/CSIRT поддержка должна быть сосредоточена на создании и обеспечении функционирования центров реагирования на инциденты в соответствии с международными стандартами. Это включает содействие в разработке стандартных операционных процедур (SOP), процессов сертификации и программ обучения.

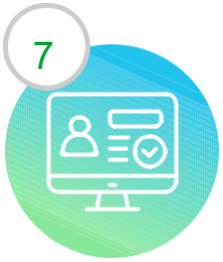
Пробелы в человеческом и техническом потенциале должны быть устранены с помощью консультативной поддержки, организованного обучения, ознакомительных поездок и предоставления технического оборудования и ноу-хау, как это наиболее целесообразно в конкретных условиях, учитывая неодинаковую готовность подразделений реагирования на инциденты в разных странах. Приоритетные направления обучения включают защиту от ICS/SCADA, аналитику угроз, анализ вредоносного ПО, обнаружение вторжений, сетевую защиту, цифровую криминалистику и юридические аспекты цифровых доказательств. Масштабируемые, стандартизированные модели обучения должны разрабатываться совместно с университетами и партнерами из частного сектора для обеспечения устойчивого притока талантов.

Для совершенствования совместных мер реагирования рекомендуется проводить межведомственные и трансграничные учения, а на местном уровне существует интерес к совместным учениям и симуляциям с заинтересованными сторонами в области кибербезопасности в Центральной Азии и их коллегами из ЕС. В дополнение к процедурной, учебной и инфраструктурной поддержке, проект может способствовать проведению технических и командно-штабных учений (национальных, межведомственных, трансграничных); помощь в создании киберполигонов; и способствовать сотрудничеству с ENISA и глобальными сообществами по реагированию на инциденты.



Повышение общественной осведомленности

Усилия по информированию общественности должны быть избирательными и адаптированными к национальным условиям. В Казахстане, где общие инициативы хорошо зарекомендовали себя, дальнейшие широкие инициативы, скорее всего, будут иметь ограниченную ценность.
С другой стороны, Узбекистан может извлечь выгоду из общенациональных кампаний по борьбе с такими распространенными угрозами, как фишинг и онлайн-мошенничество. Региональная информационно-разъяснительная работа должна быть ориентирована в первую очередь на молодежь, сельское население и государственных служащих. Партнерство с молодежными центрами и инновационными центрами для проведения интерактивных семинаров, кампаний по кибергигиене и соревнований по захвату флага может способствовать повышению цифровой грамотности и интереса к карьере в раннем возрасте. Следует поощрять стандартизированное обучение государственных служащих кибергигиене; Там, где это возможно, существующие платформы электронного обучения, такие как AIstudy.uz Узбекистана, должны быть расширены для этой цели. Согласование информационно-разъяснительной работы с международными инициативами (например, Месяцем осведомленности о кибербезопасности) может повысить как доверие, так и влияние. Органы власти также должны поощрять государственно-частное сотрудничество и сотрудничество в этих областях, а также координировать усилия по повышению осведомленности для максимизации их воздействия без дублирования уже существующих кампаний. Институциональные партнерские отношения между правительствами, академическими кругами и гражданским обществом должны быть формализованы в целях обеспечения преемственности и снижения зависимости от внешних грантов.



Развитие киберобразования

Усилия по расширению киберобразования должны быть направлены на повышение академического потенциала и модернизацию учебных программ. Введение модулей по кибербезопасности в школьные и университетские ИТ-программы, а также интеграция форматов обучения на основе практических задач (challenge-based learning) помогут сформировать базовые знания и практические навыки. Особое внимание следует уделить укреплению программ бакалавриата и магистратуры, а также подготовке выпускников, готовых к трудоустройству как в государственном, так и в частном секторах. Необходимо формализовать сотрудничество между образовательными учреждениями и агентствами по кибербезопасности, особенно в части совместной разработки учебных программ и обмена преподавательским составом.

Разработка учебных программ и форматов обучения выиграет от технической помощи и сотрудничества с академическими и учебными учреждениями ЕС. Учебные визиты в ЕС и обмены преподавателями для обмена методологиями преподавания и исследовательскими практиками могут стать отправной точкой для более глубокого сотрудничества и академического партнерства.

Развитие кадрового потенциала

Для формирования устойчивого кадрового потенциала необходимо расширять практические и инклюзивные возможности обучения, ориентированные на потребности рынка труда. Следует продвигать программы, ориентированные на трудоспособное взрослое население и повышение квалификации ИТ-специалистов, наряду с национальными инициативами по привлечению иностранных экспертов и переподготовке отечественных талантов. Международные форумы, такие как Kood/Jõhvi в Эстонии, предлагают адаптируемые модели для обучения взрослых кибербезопасности. Структурированное сотрудничество с академическими и учебными заведениями ЕС будет иметь ключевое значение для разработки учебных программ и проведения обучения. Наконец, региональные и международные форумы, в том числе конференции по кибербезопасности, должны использоваться для ознакомления с передовым мировым опытом, двустороннего взаимодействия, политического диалога и повышения наглядности национальных усилий.

Сосредоточив внимание на этих ключевых областях – стратегической согласованности, правовой ясности, укреплении институтов и координации, защите КИИ, реагировании на инциденты, адресной осведомленности и развитии трудовых ресурсов – страны Центральной Азии могли бы значительно укрепить свою национальную кибербезопасность. Поддержка проекта может усилить и поддержать эти усилия, помочь устранить пробелы в потенциале и привести региональные подходы в соответствие с передовой практикой ЕС и международным опытом.

e-Governance Academy
Ahtri 6, 10151 Tallinn, Estonia
+372 663 1500 | info@ega.ee | ega.ee
Facebook, LinkedIn: egovacademy