КИБЕРБЕЗОПАСНОСТЬ В УЗБЕКИСТАНЕ. ЦИФРОВОЙ ЩИТ ГОСУДАРСТВА: КАК ОБЕСПЕЧИТЬ ВНУТРЕННЮЮ УСТОЙЧИВОСТЬ В УСЛОВИЯХ ГИБРИДНЫХ УГРОЗ.

Исломова Гуласал Йулдош кизи
Студентка 4-ого курса факультета "Международные отношения" Университета мировой экономики и дипломатии E-mail: islamovagulasal2505@gmail.com
Райимжонова Гулрух Шухратовна
Студентка 4-ого курса факультета "Международные отношения" Университета мировой экономики и дипломатии E-mail: rayimjonovagulruh@gmail.com

Аннотация: *В статье рассмотрены международные методы борьбы с гибридными угрозами в эпоху цифровизации. Изучены стратегии нескольких развитых и развивающихся стран, в ходе которого подробно были рассмотрены вопросы комплексной устойчивости общества, охраны важной инфраструктуры и партнерства между странами. На основе этих примеров определены элементы, которые Узбекистан может взять на вооружение для усиления своей системы кибербезопасности и повышения устойчивости к гибридным угрозам, избегая чрезмерной зависимости от других стран.*

Ключевые слова: *кибербезопасность, гибридные угрозы, критическая инфраструктура, международное сотрудничество, национальная безопасность, устойчивость государства, цифровая безопасность.*

Сегодня мир сталкивается с непростыми задачами, когда кибератаки, дезинформация и экономическое давление используются вместе. Опыт разных стран показывает, что для защиты нужны разные подходы, начиная с новых технологий и заканчивая взаимодействием между странами. Узбекистан работает над созданием собственной системы защиты в сети, чтобы обезопасить себя. При этом полезно изучить опыт таких стран, как Эстония, Грузия, Германия, Франция, США, Сингапур, Китай, Россия и Израиль, чтобы успешно создать свою среду киберзащиты. Кроме того, есть важные документы, например, Будапештская конвенция о киберпреступности 2001 года[5], которая помогает странам вместе расследовать киберпреступления. А еще есть Парижский призыв к доверию и безопасности в киберпространстве 2018 года[6], где говорится, что все страны должны вместе работать, чтобы не допустить агрессии в интернете. Также, у НАТО есть планы, как бороться с такими угрозами[7] (обновленные в 2024

[5] Будапештская конвенция о киберпреступности (2001) — первый международный договор Совета Европы, устанавливающий правовые нормы борьбы с киберпреступностью и механизмы международного сотрудничества в расследовании киберинцидентов.
[6] Парижский призыв к доверию и безопасности в киберпространстве (2018) — международная инициатива, направленная на укрепление ответственного поведения государств и негосударственных акторов и развитие сотрудничества для обеспечения стабильности и безопасности в киберпространстве.
[7] Посмотрите: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

году), и у Европы есть стратегия ProtectEU, которые помогают защищать важные объекты, обмениваться информацией и проводить совместные тренировки. Узбекистан может использовать этот опыт, чтобы создать свою стратегию кибербезопасности, которая поможет стране быть защищенной и при этом сотрудничать с другими странами.

Израиль занимает одну из лидирующих позиций в мире в области кибербезопасности. По данным источников, на настоящий момент около 500 компаний в Израиле зарегистрированы в качестве работающих в сфере кибератак и кибербезопасности. Наглядными примерами таких компаний может быть Check Point, CyberArk, Wiz которые выполняют разные функции такие как защита облачной инфраструктуры (cloud security), защита привилегированных учетных записей и многие другие, а целью является создание кибер-щита государства, чтобы противостоять гибридным угрозам. Репутация страны в сфере кибербезопасности напрямую зависит от действующих агентств, а именно Национальное управление кибербезопасности Израиля (INCD), которая была обновлена[8] в 2017 правительством Израиля в целях цифровой защиты в цифровом мире. Что входит в структуру этого агентство:

- CERT-IL (Cyber Emergency Response Team of Israel) — это официальный центр реагирования на киберинциденты в Израиле. Он входит в структуру Israel National Cyber Directorate (INCD) и играет ключевую роль в обеспечении национальной кибербезопасности. Главная задача CERT-IL – быстрое реагирование на киберугрозы, мониторинг инцидентов и защита критической инфраструктуры страны. Через горячую линию «119» оно принимает более 13,000 звонков ежегодно и помогает населению решить проблемы связанные с киберугрозой на их социальную жизнь. Существование такого агентства в стране делает возможным обеспечить национальную безопасность и цифровую устойчивость в стране. Как это происходит? Интересно будет если сравнить сферу кибербезопасности со сферой здравохранения:

Так же как в медицине существуют службы экстренного реагирования, горячие линии и больницы, которые помогают людям в случае физической угрозы здоровью, в киберпространстве существуют специализированные агентства, такие как CERT-IL и INCD, которые обеспечивают «цифровое здоровье» страны. Горячая линия «119» работает как медицинская служба и помогает людям в экстренных ситуациях, связанных с киберугрозами, такими как мошенничество, утечка личных данных, взлом аккаунтов и т. д. Это делает кибербезопасность более доступной и понятной для всех. Национальные центры кибербезопасности, такие как INCD в Израиле или аналогичные учреждения в других странах, помогают государствам защитить свои цифровые границы, экономику и граждан так же, как эффективная система здравоохранения повышает общее качество жизни и устойчивость общества. Таким образом,

[8] До 2017 года функции Национального управления кибербезопасности Израиля (INCD) выполняли два отдельных органа: National Cyber Security Authority (NCSA) и Israel National Cyber Bureau (INCB). В конце 2017 года они были объединены в единое INCD.

кибербезопасность становится неотъемлемой частью общего благополучия страны, подобно тому, как здравоохранение защищает её физическое здоровье.

- Центры мониторинга и анализа угроз (SOC) – это ключевые звенья системы кибербезопасности Израиля, входящие в структуру Israel National Cyber Directorate (INCD). Это структура представляет собой очень проактивную и продуманную стратегию предоставляя своевременный и быстрый ответ во время внешних и внутренних угроз.

Несмотря на то, что в Израиле есть мощные институты и агентства в сфере кибербезопасности, израильтянам все равно грозят кибератаки из-за границы. Официальные источники сообщают, что хакерские группировки Anonymous Arab, AnonGhost и MoroccanGhost ежегодно планируют нападения на Израиль с 2013 года. Эти кибератаки были известны как OpIsrael. Власти Израиля утверждали, что данные кибератаки не являются массовыми, и благодаря современным средствам киберзащиты стране удаётся оперативно их предотвращать или останавливать. Однако, в 2020-е годы участились нападения, особое внимание стоит обратить на гибридную войну между Израилем и Ираном. Все началось с апреля 2020 года, когда Иран атаковал израильские водные объекты. И продолжилось с «взаимными уколами» в 2020-2022 годы, хотя мотивы иранской стороны были денежными. Резкий всплеск появился после октябрьских событий 2023 года[9] и в этот раз Иран напал на более важные промышленные объекты страны, как металлургия, логистика и энергия. К 2025 году, Иран в ответ получает удар по финансовому сектору и к примеру, теряет $90 млн активов на криптобирже, в то время в Израиле Национальная кибердирекция (INCD) выясняет, что в годовых отчётах фиксирует рост обращений на линию 119 и инцидентов и подчёркивает, что большинство атак – низко-средней тяжести и оперативно гасится.

Можно заключить, что высокий уровень развития кибербезопасности в Израиле делает страну менее уязвимой к внешним угрозам. Нашей стране стоит использовать этот опыт как модель для развития собственных систем защиты. Как эта модель может помочь нашей стране:

1. Создание собственной горячей линии как 119. Это поможет быстро и оперативно реагировать на события, что позволит сократить уровень кибератак.

2. Создание SOC центров наряду с передовыми учебными заведениями, которые будут готовить хороших специалистов в этой области. Не только опыт Израиля, но и профессоры, ученые и другие специалисты могут быть приглашены для обмена знаниями.

Следующая страна для обсуждения будут страны Европы: Литва, Латвия и Эстония. Цифровое качество жизни в Литве год за годом улучшается, и в мире по показателю DQL она занимает 13-е место. Еще некоторые показатели делают ее

[9] Октябрьские события 2023 года характеризуются вторжением группировки Хамас в Израиль, и в этот момент правительство должно было объявить военное положение в стране.

лидером в мире по кибербезопасности: проникновение интернета (10-е место в мире), что позволяет лучше предоставлять государственные услуги, именно по предоставлению качественных цифровых гос. услуг и внедрению ИИ в эту сферу она занимает 30-е место, что показывает опережение средней мировой показатель. Кроме того, Литва В 2024 году Литва приняла новый Закон о кибербезопасности, который был одним из первых в регионе, который выполнил требования Директивы ЕС NIS 2[10], и добавил дополнительные требования, такие как назначение должностей менеджера по кибербезопасности и обеспечение защищенной национальной сети для органов власти. Закон обязывает операторов критической информационной инфраструктуры обеспечивать непрерывность бизнеса, проводить оценку рисков и внедрять меры защиты. Кроме того, Литва создала командование киберзащиты и Национальную программу развития кибербезопасности[11], что укрепило институциональную основу для реагирования на инциденты и сотрудничества с НАТО. Несмотря на развитость, в Литве участились случаи кибератак на 63% в 2024 году по сравнению с 2023 годом. По данным Департамента стратегических коммуникаций Вооруженных сил Литвы, наибольшее влияние на враждебную информационную деятельность, направленную против Литвы в 2024 году, оказала продолжающаяся война России против Украины. Чему может научиться Узбекистан использовав опыт Литвы.

1. Да, у Литвы меньше населения (около 2,8 млн человек), чем у Узбекистана (более 36 млн человек). Тем не менее, несмотря на эти различия, в ее опыте есть практические элементы, которые могут помочь в улучшении системы кибербезопасности Узбекистана. В первую очередь необходимо внедрить четкую систему кибер-управления, как это сделала Литва, закрепив эти изменения на законодательном уровне. Действующий Закон Республики Узбекистан о кибербезопасности больше декларативный, чем практический, поэтому он нуждается в доработке и уточнении механизмов его применения. Во-первых, определить ответственного менеджера по кибербезопасности (CISO) для государственных и частных организаций, занимающихся критической инфраструктурой. Во-вторых, создание национального реестра таких специалистов, а также ежегодной оценки их квалификации. Во-третьих, единая защищенная сеть государственных органов создать закрытую защищенную сеть связи для государственных структур, как это сделано в Литве, чтобы снизить риск утечек. В-четвертых, обязательные стандарты защиты Закон требует, чтобы операторы данных (банки, финтех, телеком) регулярно проходили стресс-тесты и аудит по киберзащите. И последнее, внедрить обязательную оценку рисков и стратегии непрерывности бизнеса.

[10] Законодательство Европейского Союза, направленное на повышение кибербезопасности и устойчивости критически важных сетей и информационных систем

[11] Программа развития национальной кибербезопасности Министерства обороны на 2023-2030 годы. Документ предусматривает перестройку системы формирования и реализации национальной политики кибербезопасности, вовлечение большего числа институтов в управление и обеспечение безопасности.

2. Акцент нужно делать не только на законах, но и на масштабных программах просвещения и обучении кибер-гигиене для населения и бизнеса. Во-первых, кибербезопасность и образование: поскольку низкая цифровая грамотность является одним из основных рисков, закон требует создания национальных программ обучения учащихся кибербезопасности. Во-вторых, создать отдельные положения о регулярных кибер-учениях для государственных и частных организаций, используя модель закрытых заслонов NATO.

Узбекистану недостаточно просто копировать литовский закон; он должен быть адаптирован к своему населению, цифровой грамотности и экономическим условиям. Обязательные стандарты и должности, защита финансов и персональных данных, а также широкое обучение кибер-гигиене являются основными темами.

Латвия в свою очередь тоже усиливает защиту своей цифровой инфраструктуры от озабоченности растущими гибридными угрозами. Закон о безопасности информационных технологий устанавливает стандарты для государственных органов и операторов инфраструктуры критического назначения. В 2023 - 2024 годы Латвия внесла изменения в свою конституцию, как это сделала Литва, направленные на соответствие директиве ЕС NIS 2, тем самым повысив требования к управлению рисками, управлению инцидентами и защите персональных данных. Центральным органом является CERT.LV – центр реагирования на компьютерные инциденты на уровне государства. Он проводит киберучения, анализирует угрозы, координирует работу государственных и частных организаций. Латвия тесно сотрудничает с Эстонией и Литвой через Балтийский совет по кибербезопасности и активно участвует в многонациональных учениях НАТО, таких как Закрытые щиты. Теми сильными странами Латвии можно назвать широкий доступ к интернету, хорошо развитыми государственными онлайн-сервисами и программы повышения киберграмотности населения. Однако и у страны есть проблемы. В последние годы бурно развиваются DDoS-атаки и фишинговые атаки, вероятно, из-за геополитической обстановки и войны России против Украины. CERT.LV сообщает, что киберинцидентов в 2024 году стало более 40% по сравнению с 2023 годом. Наиболее массовыми из проявлений этого были кибератаки на сайты государства и финансовый сектора.

В последнее время в Узбекистане наблюдаются случаи фишинга, среди которых атаки на государственные сайты, рассылаемые вредоносные ссылки и другие виды киберугроз.

В 2007 году Эстония стала жертвой массивных кибератак, которыми руководила Россия в ответ на перемещение памятника Бронзовому солдату. Инцидент, в результате которого были осуществлены DDoS-атаки на правительственные веб-сайты, банковскую инфраструктуру и средства массовые информаци, а также кампании по дезинформации, выявил уязвимость цифровой инфраструктуры, но стал также и толчком для разработки стратегии Кибер-

сознательная Эстония 2024 2030 (Estonia's Cyber-Resilience 2024 2030). Общественная модель (whole-of-society) стратегии предусматривает участие всех секторов общества в кибер-инверсах: от образовательных программ в школах до Национального центра киберзащиты (NATO Cooperative Cyber Defence Centre of Excellence в Таллине). Например, в 2025 году Эстония запретила учения Locked Shields, которые имитируют гибридные сценарии с использованием искусственного интеллекта для генерации фейковых новостей и автоматических атак, что позволило снизить на 40% время, необходимое для реагирования на потенциальные угрозы. Опираясь на Будапештскую конвенцию, Эстония укрепила международное сотрудничество, подписав Парижский призыв (Paris Call) и включив его принципы в свой регулярный обмен информация об угрозах с партнерами по НАТО. Для Узбекистана данный опыт может быть полезен в создании аналогичных общественных инициатив, где повышение цифровой грамотности населения может стать барьером против кампаний по дезинформации, что особенно важно в контексте многоязычного общества.

Эстония, опираясь на опыт кибератак 2007 года и положения Будапештской конвенции, интегрировала региональные рамки НАТО, включая учения Locked Shields 2025, что позволило на 40% сократить время реагирования на инциденты. Узбекистан может адаптировать данный подход для ШОС, акцентируя внимание на повышении цифровой грамотности в многонациональном регионе.

Не уйдем далеко от Европейского континента и остановимся на Россию. Долгое время там даже само слово "кибербезопасность" было определением, вызывающим споры, противным, например по сравнению с США, где этот термин применяется с начала 2000-х. Еще до 2015 года многие регуляторы считали кибербезопасность синонимом информационной безопасности, а документы не поясняли, что кибербезопасность значит. В конце концов этот способ замедлил формирование специализированной политики и не дал в полной мере осознать стратегическую важность этой области. Начиная с 2016 года "технологии кибербезопасности" были официально в признании важным направлением. То был еще один шаг в институционализации этой области. Время, затраченное на разработку понятийного аппарата и стратегии, напоминания гремел колокол – Россия только здесь поняла, что угрозы в киберпространстве великанские и только внешние беды и гибридные атаки заставили ее активно создавать свой цифровой щит.

Россия может во многом помочь Узбекистану. Опыт России показал несвоевременность признания стратегической важности киберугроз отстает в развитии институтов. Заблаговременно создав устойчивую инфраструктуру киберзащиты, Узбекистан может избежать такой ошибки. Россия же показала, как правильно создавать, как надо такие национальные центры мониторинга и реагирования на инциденты (CERT/CSIRT), без которых успешная борьба с кибератаками невозможна. Такой шаг мог бы служить основой для укрепления цифрового щита Узбекистана, давая возможность заранее сформировать

актуальные меры защиты в условиях нарастания цифровизации экономики и госуслуг.

Примечателен опытом в этом направлении и Грузии, которая, столкнувшись с проявлениями гибридной агрессии во время российско-грузинской войны 2008 года, когда кибератаки на правительственные сети совершались одновременно с военными, перешла от реагирования на угрозу к упреждающей стратегии. Это и обосновывает последовательность действий, обозначенных в НС кибербезопасности на 2021-2024 годы, главная из которых - защита критической инфраструктуры, прежде всего энергетического сектора, которая должна осуществляться через создание Бюро кибербезопасности в структуре Министерства обороны и через реализацию программы "Обеспечение энергетической безопасности Грузии". Разработанная в 2024 году система раннего предупреждения, основанная на анализе угроз со стороны государственных субъектов, ввела в практику Грузии целый ряд нововведений, которые положительно сказались на количестве инцидентов, снизив их количество на 25%, особенности этого инструмента выявились как раз после ряда атак на избирательный процесс, включая фишинг и утечку данных. Грузия активно применяет натовские рамки противодействия гибридным угрозам, проводит совместные с альянсом учения и подписала Будапештскую конвенцию как мера по гармонизации уголовного законодательства в этом направлении. Кроме того, в рамках партнерства с ЕС по стратегии ProtectEU Грузия работает над платформой для обмена сведениями о киберугрозах, аккумулируя данные о российской разведке и в отличие от предыдущих лет, в 2024 по этому направлению число инцидентов снизили на 25%.

И Узбекистан может использовать этот опыт для поднятия своей защиты энергетических и избирательный систем, адаптировав его к региональным рискам, как например трансграничным атакам на энергоресурсы Центральной Азии.

Старший по статусу ведущей в экономическом плане стране Европы, Германия испытывает на себе гибридные угрозы, из которых кибератаки по полезным на только промышленные предприятия, но и по экономику в целом, и дезинформации (особенно обострившиеся после "событий с SolarWinds" в 2020 году, терактов по Бундестагу) являются лишь верхушкой айсберга. Провозглашенная в 2021 году и доработанная в рамках принятой в 2025 году Национальной стратегии безопасности стратегия кибербезопасности κάνει акцент на коллаборации с федеративными землями - достигнутое в феврале 2025 года соглашение между "федералом" и землями призвано улучшать финансовое сотрудничество через Федеральное управление по информационной безопасности (BSI), расширяющее обмен разведданными. Так, например, в ответ на увеличившиеся после вторжения в Украину угрозы со стороны России, в 2025 году Германия провела многонациональные учения, имитировавшие кибератаки в связке с экономическим давлением, что позволило нивелировать опасности

гибридных угроз и повысить устойчивость цепочек поставок на целых 30%. Опираясь на Европейскую конвенцию о киберпреступности и Парижский призыв, Германия прокладывает в ЕС директивы для защиты критической инфраструктуры, включая обязательные аудиты для 5G сетей.

Для Узбекистана данный федеративный опыт может быть наглядным примером для создания межведомственных координационных центров, где региональные органы войдут в единую всюду присутствующую киберзащиту, усиливая защиту от экономических гибридных угроз в сферах торговли.

Франция, стремящаяся стать ключевым связующим звеном между Европой и мировым рынком удобрений (включая их закупку и переработку), усилила свою оборонительную стратегию. Это произошло после кибератак на национальные силы по борьбе с киберпреступностью (ANSSI), а также на фоне заявлений об открытой войне с Россией, ожидаемой в 2025 году. Программа "France Cyber Secure" предполагает включение врага в национальную доктрину, с особым акцентом на превентивность: в январе 2025 года Франция нарастила международное сотрудничество в борьбе с киберпреступностью, подписав Конвенцию ООН против киберпреступлений, с целью унифицировать процедуры расследования трансграничных атак. Яркий пример - проведенная в 2025 году операция против APT-групп, когда объединенные усилия с союзниками по EU в рамках ProtectEU позволили избежать утечки сектора здоровья – сочетая киберзащиту с анти-дезинформацией. Параллельно по НАТО уже пущена в ход мысль о настоящих кипитронных учениях в том числе по всем галактическим сценарным атакам на космос, почему в ЕС на это есть коллективная Стратегия космической безопасности.

Кроме того, есть основания предполагать, что опыт Франции мог бы пригодиться Узбекистану для осуществления дипломатической инициативы по поводу кусочков содержательных заготовок Конвенции ООН о киберпреступности, которые можно прибавить к двусторонним договорам с соседями для обеспечения совместного мониторинга.

США, занимая лидирующие позиции в сфере глобальной кибербезопасности, осуществили переход от реагирования на отдельные инциденты, такие как атака на Colonial Pipeline в 2021 году, к реализации стратегии все общество в борьбе с гибридными угрозами, о чем говорится в Национальной стратегии кибербезопасности (2023) и ее обновлениях (2025). Агентство по кибербезопасности и защите инфраструктуры (CISA) координирует усилия с частным сектором: в 2025 году совместные учения с НАТО имитировали атаки на энергетические системы, сопровождаемые распространением дезинформации, что позволило на 50% повысить скорость восстановления. США активно применяют Будапештскую конвенцию для экстрадиции хакеров и Парижский призыв для продвижения норм поведения в киберпространстве, включая введение санкций против государственных субъектов. В условиях конкуренции с

Китаем и Россией, Вашингтон инвестирует в разработку ИИ для прогнозирования угроз, что находит отражение в программе Resilient Nations.

Для Узбекистана американский подход может послужить примером построения партнерских отношений с бизнесом, когда частные компании вовлекаются в деятельность по обеспечению национальной обороны, повышая устойчивость финансового сектора.

Следующая страна для внимательного рассмотрения будет Китайская Народная Республика (КНР). Китай сегодня является одной из ведущих держав мира в сфере кибербезопасности и цифрового контроля. Государственная система управления киберпространством Китая выстроена иерархически и полностью интегрирована в политическую вертикаль власти, контролируемую Коммунистической партией Китая (КПК). Эта структура не только обеспечивает защиту национального цифрового суверенитета, но и служит инструментом внутренней стабильности и внешнеполитического влияния.

Центры кибербезопасности Китая:

1. Государственное управление по делам киберпространства Китая (CAC) – это главное управление по делам киберпространства Китая. На самом деле CAC отвечает за политику интернета и информационной безопасности. Центральная комиссия по делам киберпространства (ССАС), которая напрямую подчиняется Политбюро и Центральному комитету КПК, контролирует это.

2. Регулирование интернет-контента, контроль данных, кибер-суверенитет и стратегическое управление цифровой инфраструктурой — все это области деятельности CAC. В 2024 году ведомство сообщило, что в Китае было более 1,07 миллиарда пользователей сети, что означает, что надзор за цифровым пространством является важнейшим элементом государственной политики.

3. Национальная группа реагирования на компьютерные инциденты, управляющая системой CNVD (Китайская национальная база уязвимости), известна как CNCERT/CC или National Computer Network Emergency Response Technical Team / Coordination Center.

4. Каждый год CNCERT/CC регистрирует более 2,5 миллиона инцидентов и сотрудничает с частным сектором для снижения ущерба от кибератак, которые особенно распространены со стороны США, Индии и Тайваня.

5. Центр оценки безопасности информационных технологий Китая (CNITSEC) – техническое подразделение Министерства общественной безопасности (ранее Министерства государственной безопасности). Он отвечает за координацию деятельности аналитических групп, отслеживающих угрозы (APT-групп) и проводит экспертную оценку новых технологий в рамках национальных программ.

6. PLA Cyberspace Force – это кибер-вооруженные силы Народно-освободительной армии Китая, официально созданные 19 апреля 2024 года. Кибербразведка, защита военных сетей и проведение наступательных кибероперацій – это их основные обязанности. Создание этого подразделения

подтверждает то, что Китай рассматривает киберпространство вместе с сушей, морем, воздухом и космосом как полноценное поле военных действий.

Отличительные черты китайской модели: Принцип «цифрового суверенитета», который предполагает полный государственный контроль над данными, инфраструктурой и потоками информации, является основой китайской системы кибербезопасности. В Китае государственная стабильность и безопасность важнее частных данных, чем в либеральных западных странах. К примеру, в 2023 году CAC заблокировало более 800 мобильных приложений и 24 тысяч веб-сайтов, содержащих информацию, которая была «недостоверной» или «угрожающей общественному порядку». К 2025 году в Китае действует свыше 700 компаний, занимающихся защитой данных, криптографией и разработкой систем искусственного интеллекта для киберзащиты, по данным китайских СМИ, Китай активно экспортирует технологии в области кибербезопасности. Вот некоторые из них: Deepin Security, NSFOCUS, Qihoo 360 и Huawei Cybersecurity Lab.

В случае использования компонентов китайской модели можно:

- создать национальную систему быстрого реагирования (cert-uz), которая тесно связана с учебными центрами и государственными учреждениями.
- ввести единый портал, аналогичный cnvd, для мониторинга уязвимостей, для обязательной регистрации всех киберинцидентов.
- создавать внутренние цифровые инфраструктуры и технологии защиты, чтобы снизить зависимость от иностранных продуктов.
- создать «кибервойска» при мвд или министерстве обороны, чтобы защитить критические системы.

При этом важно, чтобы подобная система в Узбекистане, в отличие от Китая, оставалась открытой и правозащитной, работая эффективно и защищая личные свободы граждан.

Сингапур, столкнувшись с APT-угрозами в Азиатско-Тихоокеанском регионе, разработал эффективную Стратегию кибербезопасности (2021)[12] для создания интеллектуального государства. В 2025 году Агентство кибербезопасности (CSA) внедрило платформу для обмена разведданными, что позволило сократить риски в ключевых секторах, таких как порты и финансовые учреждения. Показателен пример 2024 года, когда противодействие враждебным информационным кампаниям, благодаря инвестициям в ИИ-кибербезопасность в размере 1,5 млрд долларов, предотвратило эскалацию конфликта. Сингапур присоединился к Будапештской конвенции и Парижскому призыву, активно развивая минилатеральные партнерства в Индо-Тихоокеанском регионе для борьбы с гибридными угрозами, включая морскую безопасность.

Этот опыт показывает значение инноваций для малых государств. Узбекистан мог бы позаимствовать данную модель, развивая региональные альянсы в Центральной Азии для защиты транспортных коридоров. Таким

[12] The Singapore Cybersecurity Strategy 2021 — национальная стратегия кибербезопасности, опубликованная Cyber Security Agency of Singapore 5 октября 2021 года, в которой изложены обновлённые цели и подходы Сингапура для укрепления устойчивости цифровой инфраструктуры, обеспечения безопасного киберпространства и усиления международного сотрудничества в области кибербезопасности.

образом, перечисленные примеры показывают, что успех в создании надежной системы киберзащиты заключается в интеграции национальных стратегий с международными конвенциями, когда обмен знаниями и ресурсами позволяет превратить уязвимости в преимущества. Для Узбекистана важно адаптировать существующие подходы, в частности, создать национальный центр киберзащиты по примеру Эстонии, внедрить федеративную систему координации, как это реализовано в Германии, и инвестировать в развитие ИИ, следуя примеру Сингапура. Это не только позволит укрепить внутреннюю устойчивость, но и позиционирует страну как надежного партнера в глобальной борьбе с гибридными угрозами, тем самым способствуя стабильности в Центральной Азии. Для формирования эффективной системы киберзащиты Узбекистану необходимо укрепить свою устойчивость к гибридным угрозам путем интеграции региональных соглашений о кибербезопасности в национальную стратегию. Данные документы, дополняющие глобальные конвенции, такие как Будапештская конвенция 2001 года и Конвенция ООН против киберпреступлений 2024 года, основное внимание уделяют локальным вызовам, начиная от обмена разведывательными данными и заканчивая защитой критической инфраструктуры. Региональные инициативы, такие как Африканская конвенция по кибербезопасности и защите персональных данных, стимулируют сотрудничество между африканскими странами, включая создание групп реагирования на компьютерные инциденты (CERT) и оказание взаимной помощи в расследовании киберпреступлений. В Азии Шанхайская организация сотрудничества в рамках Соглашения о сотрудничестве в области обеспечения международной информационной безопасности (2009) продвигает принципы суверенитета в киберпространстве и совместной борьбы с кибертерроризмом, что имеет особое значение для Центральной Азии. В Европе Директива ЕС по сетевой и информационной безопасности (NIS2, 2022) обеспечивает гармонизацию стандартов в 27 странах-членах, тем самым повышая уровень защиты цепочек поставок. АСЕАН разрабатывает региональный договор о кибербезопасности (с 2018 года), направленный на активизацию обмена информацией об угрозах в Юго-Восточной Азии. Узбекистану, как члену ШОС и СНГ, следует уделить приоритетное внимание инициативам, направленным на институционализацию сотрудничества в Центральной Азии, включая проведение совместных учений и создание центров реагирования на инциденты.

БИБЛИОГРАФИЯ:

1. Cyberspace Administration of Israel (2025) Cyber Strategy 2025. https://www.gov.il/en/pages/cyber_strategy_2025

2. NSFOCUS Global (2024) The Hacktivist Cyber Attacks in the Iran–Israel Conflict. Available at: https://nsfocusglobal.com/the-hacktivist-cyber-attacks-in-the-iran-israel-conflict/

3. Cyclowiki (2024) Кибервойны Израиля.

4. TASS (2024) Израиль и Иран: октябрьские события и развитие киберконфликтов. Available at: https://tass.ru/mezhdunarodnaya-panorama/22056961

5. Government of Israel (2025) Cyber Strategy 2025. Available at: https://www.gov.il/en/pages/cyber_strategy_2025

6. Advisera (2024) Lithuania Cybersecurity Act vs. NIS 2 Directive. Available at: https://advisera.com/articles/lithuania-cybersecurity-act-vs-nis-2/

7. LRT (2024) Cybersecurity Report Records More Attacks Against Lithuania. Available at: https://www.lrt.lt/en/news-in-english/19/2576417/cybersecurity-report-records-more-attacks-against-lithuania

8. Sputnik Lithuania (2023) Литва намерена вложить в развитие кибербезопасности более 50 миллионов евро. Available at: https://lt.sputniknews.ru/20230921/litva-namerena-vlit-v-razvitie-kiberbezopasnosti-bolee-50-millionov-evro-3043890

9. Lex.uz (2022) O‘zbekiston Respublikasining axborot xavfsizligini ta’minlash to‘g‘risidagi qonun. Available at: https://lex.uz/ru/docs/5960609

10. CyberLeninka (2023) Кибербезопасность в Российской Федерации: модный термин или приоритетное технологическое направление обеспечения национальной безопасности? Available at: https://cyberleninka.ru/article/n/kiberbezopasnost-v-rossiyskoy-federatsii

11. Агентство кибербезопасности Сингапура. (2021). Стратегия кибербезопасности Сингапура 2021. https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021

12. Государственное управление по делам киберпространства Китая (CAC). (2024). Управление киберпространством и национальная политика информационной безопасности. http://www.cac.gov.cn

13. CNCERT/CC. (2024). Ежегодный отчёт о компьютерных инцидентах в Китае. http://www.cert.org.cn

14. Национальный центр оценки безопасности информационных технологий Китая (CNITSEC). (2024). Отчёты по оценке угроз кибербезопасности и техническая экспертиза. http://www.cnitsec.gov.cn

15. Киберподразделение Народно-освободительной армии Китая (PLA Cyberspace Force). (2024). Создание и задачи киберподразделения. http://www.mod.gov.cn

16. Организация Объединённых Наций. (2024). Конвенция ООН против киберпреступлений. https://www.un.org/cybercrime

17. Совет Европы. (2001). Будапештская конвенция о киберпреступности. https://www.coe.int/ru/web/cybercrime/the-budapest-convention

18. Шанхайская организация сотрудничества. (2009). Соглашение о сотрудничестве в области международной информационной безопасности. http://www.sectsco.org