Политика / Politics

Политика Республики Корея по обеспечению кибербезопасности: цели, инструменты, международное сотрудничество

 DOI: 10.31857/S0131281225010016

Волощак Валентин Игоревич

Кандидат исторических наук, научный сотрудник Лаборатории Азиатских и Тихоокеанских исследований, Институт истории, археологии и этнографии народов Дальнего Востока Дальневосточного отделения РАН (адрес: 690001, Приморский край, Владивосток, Пушкинская ул., 89). ORCID: 0000–0001–7557–7494. E-mail: v.voloshchak@ihaefe.ru

Статья поступила в редакцию 16.12.2024.

Аннотация:

Статья посвящена анализу основных направлений политики Республики Корея по обеспечению кибербезопасности после прихода к власти в 2022 г. администрации Юн Сок Ёля. На основе анализа официальных документов РК, включая новую редакцию Стратегии кибербезопасности 2024 г., автор показывает, что основным аспектом «проактивной» политики Юн Сок Ёля является апелляция к фактору северокорейской киберугрозы, что обусловливает необходимость развития наступательного киберпотенциала и превентивного реагирования на киберугрозы. Автор также отмечает, что за последние три года Южная Корея расширила свое участие в международных учениях по кибербезопасности (в том числе под эгидой НАТО) и в целом укрепила сотрудничество в области кибербезопасности со многими зарубежными партнерами. Наконец, важной частью политики по обеспечению кибербезопасности является реформирование процесса управления деятельности государственных и частных организаций сектора кибербезопасности, направленное на увеличение роли Национальной разведывательной службы и создание единого координационного органа — т.н. Национального комитета кибербезопасности. Автор заключает, что в условиях противодействия оппозиции, не согласной с политикой централизации и считающей, что усиление роли Национальной разведывательной службы в вопросах обеспечения национальной кибербезопасности является злоупотреблением властью и ведет к нарушениям прав человека, Юн Сок Ёлю не удалось реализовать главную инициативу своей политики кибербезопасности и принять Общий закон «О кибербезопасности». При этом данная ситуация практически идентична попыткам администрации Пак Кын Хе принять Закон «О кибертерроризме», также подразумевавший расширение сферы полномочий разведки и впоследствии заблокированный оппозиционной фракцией.

Ключевые слова:

кибербезопасность, Республика Корея, стратегия, разведка, централизация, киберугрозы, реформа.

Источники финансирования:

Статья подготовлена в рамках темы государственного задания 1023110200001–7–5.6.1 «Азиатско-Тихоокеанский регион в условиях соперничества Запада и Большого Востока за формирование нового мирового порядка».

Для цитирования:

Волощак В.И. Политика Республики Корея по обеспечению кибербезопасности: цели, инструменты, международное сотрудничество // Проблемы Дальнего Востока. 2025. № 1. С. 7–22. DOI: 10.31857/S0131281225010016.

Пришедшая к власти в 2022 г. администрация президента Юн Сок Ёля не обошла вниманием вопросы обеспечения кибербезопасности. Более того, проблемы кибербезопасности заняли достаточно важное место в риторике президента[1] и в стратегических документах Республики Корея (РК), став за последние несколько лет одним из значимых аспектов межкорейского противостояния[2] и внутриполитической дискуссии между правительством и оппозицией[3]. В этих условиях администрация Юн Сок Ёля пытается проводить «проактивную» политику по обеспечению кибербезопасности, направленную на противодействие КНДР, укрепление международного сотрудничества и централизацию процесса управления государственными и частными организациями сектора кибербезопасности.

Кибербезопасность в стратегических документах Республики Корея

В докладе «120 задач государственной политики правительства Юн Сок Ёля» (июль 2022 г.), обозначившем основные приоритеты и целевые показатели внутренней и внешней политики государства на пятилетний срок, выделена отдельная задача № 101 «Укрепление национального потенциала реагирования на угрозы кибербезопасности». Ответственными за реализацию задачи назначены Министерство науки и информационно-коммуникационных технологий, Министерство обороны, Министерство иностранных дел, а также Национальная разведывательная служба (НРС). В основные цели задачи № 101 входит создание парадигмы кибербезопасности для реагирования на киберугрозы, исходящие от государственных и негосударственных хакерских организаций, поддержка безопасной киберсреды для граждан и бизнеса, консолидация сотрудничества и поддержка конкуренции релевантных организаций на правительственном уровне, развитие человеческих ресурсов[4].

Центральной инициативой в рамках работы по реализации заявленных целей провозглашено создание Национального комитета кибербезопасности — специального органа, который выступит «контрольной башней» и будет координировать работу всех государственных и негосударственных ведомств и организаций, работающих в области информационной и кибербезопасности. Другой задачей заявлено создание защищенной от кибератак «цифровой платформы» общественной инфраструктуры (умные сети электроснабжения и др.).

Развитие сектора кибербезопасности перекликается также и со смежными государственными планами, такими как задача № 75 «Войти в топ-5 глобальных лидеров в области науки и технологий посредством развития прорывных стратегических технологий». Задача предполагает правительственную поддержку развития стратегических технологий, в списке которых технологии кибербезопасности указаны наряду с полупроводниками, ядерными электростанциями нового поколения, водородной энергетикой, технологиями 5G и 6G, робототехникой и искусственным интеллектом, квантовыми технологиями и др. Задача № 78 «Создание лучшей в мире сети связи и ускорение внедрения цифровых инноваций» провозглашает развитие инфраструктуры 5G и 6G, повышение

---

[1] *Kim Eun-jung*. Yoon urges enhanced cybersecurity against state-sponsored hacking attacks // *Yonhap*. August 27, 2024. URL: https://en.yna.co.kr/view/AE№ 20240827005400315 (дата обращения: 14.12.2024).

[2] *Jeong Yeonoh, Choi Jin-Young, Park Seunghyun*. Improvement of the Defense Planning and Management System to Implement the ROK's National Cybersecurity Strategy // *The Korean Journal of Defense Analysis*. 2023. Vol. 35. No. 3. Pp. 338–339.

[3] *Волощак В.И.* Проблемы развития национальной системы кибербезопасности Республики Корея // *Проблемы Дальнего Востока*. 2018. № 3. С. 122.

[4] 윤석열 정부 120대 국정 과제 [120 задач государственной политики правительства Юн Сок Ёля]. 서울: 대한민국정부, 2022. 168쪽.

стабильности и защищенности сетей, поддержку конкурентоспособности южнокорейских компаний на рынке связи[5]. В целях развития человеческого потенциала в области кибербезопасности правительство Юн Сок Ёля инициировало образовательную программу «100 тысяч киберталантов», предполагающую сотрудничество университетов, специализированных образовательных центров (а также открытие новых региональных центров). Подготовленные в них кадры мыслятся как «резервные киберсилы» государства[6].

Наконец, совершенствование системы кибербезопасности Южной Кореи имеет важное значение с точки зрения задач национальной обороны. Основным их приоритетом является сдерживание развития и использования Северной Кореей ракетного и ядерного оружия, дальнобойной артиллерии, а также противодействие кибероперациям, предположительно проводимым северокорейскими подразделениями. Согласно задаче № 104 «Значительное укрепление потенциала реагирования на ракетно-ядерную угрозу КНДР» РК намерена образовать новое стратегическое командование, ответственное за проведение интегрированных операций, подразумевающих использование средств кибер и радиоэлектронной борьбы, ракетного и высокоточного оружия в целях сдерживания различных угроз со стороны КНДР[7].

1 февраля 2024 г. Южная Корея опубликовала новую Стратегию кибербезопасности, которая была сразу охарактеризована в СМИ как более «наступательная» по сравнению с предыдущей редакцией 2019 г.[8] Стратегия кратко дает определение кибербезопасности, характеризует спектр киберугроз, актуальных для государства, и формулирует пять стратегических направлений политики кибербезопасности для Южной Кореи.

Под кибербезопасностью в Стратегии понимается защита государства, граждан и национальных интересов путем выявления, проверки и блокирования киберактивностей, направленных против национальной безопасности и национальных интересов со стороны угрожающих акторов, таких как Северная Корея, а также разработка и реализация необходимых контрмер[9].

КНДР отдельно упоминается и в характеристике киберугроз, актуальных для Южной Кореи. К таковым Стратегия относит утечку передовых технологий, кражу виртуальных активов, манипулирование общественным мнением путем распространения ложной информации и «фейковых» новостей, нейтрализацию работы критической инфраструктуры вследствие кибератак. Согласно документу, данные угрозы могут исходить от т.н. акторов киберугроз — международных или поддерживаемых отдельными государствами хакерских организаций. В качестве примера такого государства приводится Северная Корея, которая «сегодня развивает потенциал своих кибератак, способных оказать разрушительное воздействие на военную, финансовую, информационную инфраструктуру, обходит международные санкции с помощью незаконной киберактивности и собирает средства для ракетно-ядерных разработок»[10].

---

[5] 윤석열 정부 120대 국정 과제 [120 задач государственной политики правительства Юн Сок Ёля]. 서울: 대한민국정부, 2022. 131쪽.

[6] 윤석열 정부 120대 국정 과제 [120 задач государственной политики правительства Юн Сок Ёля]. 서울: 대한민국정부, 2022. 168쪽.

[7] 윤석열 정부 120대 국정 과제 [120 задач государственной политики правительства Юн Сок Ёля]. 서울: 대한민국정부, 2022. 174쪽.

[8] *Lee Haye-ah*. Gov't unveils Nat'l Cybersecurity Strategy with new focus on N. Korea // *Yonhap*. Febraury 1, 2024. URL: https://en.yna.co.kr/view/AE№ 20240201007800315 (дата обращения: 14.12.2024).

[9] 국가 사이버안보 전략 [Национальная стратегия кибербезопасности]. 서울: 대통령실 국가안보실, 2024. 11쪽.

[10] 국가 사이버안보 전략 [Национальная стратегия кибербезопасности]. 서울: 대통령실 국가안보실, 2024. 11쪽.

Стратегия кибербезопасности формулирует три ключевые цели[11]:

1. Развитие наступательной кибероборонbы — переход к парадигме наступательного реагирования на киберугрозы в условиях их усложнения и разнообразия.

2. Укрепление глобального лидерства — усиление сдерживания киберугроз за счет установления партнерств с отдельными государствами, а также укрепление международного сотрудничества и солидарности, включая развитие норм ответственного поведения в киберпространстве.

3. Обеспечение надежной кибероборонbы — развитие инфраструктуры кибербезопасности на общегосударственном уровне, которая позволит не только бороться с внешними угрозами кибербезопасности, но и предотвращать сбои информационных сетей, защищая повседневную цифровую жизнь граждан.

Во исполнение этих целей обозначены пять стратегических направлений[12]:

1. Укрепление наступательного потенциала кибероборонbы. Данный вектор является одним из ключевых в политике кибербезопасности Юн Сок Ёля и призван отразить акцент на факторе Северной Кореи — главном акторе киберугроз, источнике распространения ложной информации и организатора операций влияния, способных, с точки зрения РК, вызвать «социально-экономический хаос и раскол общественного мнения». В рамках развития наступательного элемента стратегии кибербезопасности предполагается разработать руководящие принципы сдерживания угроз национальной безопасности в киберпространстве для координации работы различных государственных ведомств и частных организаций, работающих в области кибербезопасности. Больше внимания предполагается также уделять разведывательной деятельности. В связи с этим вооруженным силам и НРС РК отведена задача выявления и анализа источников кибератак, превентивного и жесткого реагирования на них, подготовки к ожидаемым атакам, а также своевременной передачи информации релевантным органам государственной власти. Работа по сбору разведданных НРС должна стать частью общенациональной политики по сбору, анализу и обмену информацией о киберугрозах как между южнокорейскими ведомствами, так и с государствами, с которыми РК развивает сотрудничество в области кибербезопасности.

2. Установление глобальной системы сотрудничества в сфере кибербезопасности. Приоритетом Южной Кореи является развитие международного сотрудничества в области кибербезопасности со странами, «которые разделяют ценности свободы, открытости, мира и безопасности в киберпространстве». В числе главных партнеров обозначены США и Великобритания, с которыми Южная Корея уже имеет соглашения — о создании «Стратегической структуры сотрудничества в области кибербезопасности» с Вашингтоном и о «Стратегическом киберпартнерстве» с Лондоном. Помимо цели на углубление сотрудничества и взаимной «проактивной» поддержки в реагировании на киберугрозы с этими партнерами, РК выделила также и ряд партнеров второго приоритета — блок НАТО, Австралия, Канада и Индия, с которыми предполагается расширить обмен технологиями и информацией о киберугрозах. Также Южная Корея выступает за создание международного многостороннего соглашения по реагированию на киберпреступления и в целом продвигает развитие диалога по информации о киберугрозах, технологиям безопасности и другим направлениям на основе взаимодействия между государственными органами, частными компаниями и в рамках каналов «полуторного трека».

---

[11] 국가 사이버안보 전략 [Национальная стратегия кибербезопасности]. 서울: 대통령실 국가안보실, 2024. 17–18쪽.

[12] 국가 사이버안보 전략 [Национальная стратегия кибербезопасности]. 서울: 대통령실 국가안보실, 2024. 20–33쪽.

3. Укрепление кибербезопасности общественной инфраструктуры государства. Важной частью политики кибербезопасности РК названы поддержка минимальных требований безопасности, покрывающая жизненный цикл основных объектов общественной инфраструктуры, и постоянная готовность обеспечить техническую поддержку. Для этого предполагается создать общегосударственную интегрированную систему мониторинга и восстановления объектов общественной инфраструктуры, разработать систему обнаружения продвинутых кибератак. Планируется также реформирование процессов управления данными на цифровых правительственных платформах — внедрение подхода «нулевого доверия» и обеспечения видимости информации об идентификационных данных. Для создания условий бесперебойной и надежной работы государственных цифровых платформ РК также планирует укреплять безопасность цепочек поставок IT-продуктов и технологий, предпринимать меры по выбору надежных партнеров. Наконец, важным аспектом обеспечения кибербезопасности общественной инфраструктуры является обновление соответствующего законодательства, уточнение стандартов и типологизация киберинцидентов, стандартизация информации о конфигурации программного обеспечения для минимизации уязвимостей цифровых платформ и сервисов.

4. Обеспечение конкурентного преимущества в новых технологиях. Одной из обозначенных целей РК является обеспечение защиты от новых угроз, вызванных распространением квантовых технологий, искусственного интеллекта и т.д. путем увеличения бюджета на НИОКР в области новых технологий, в т.ч. применительно к сфере кибербезопасности. Среди запланированных мероприятий обозначены создание специальной организации, ответственной за разработку, обмен и трансфер высоких технологий в области кибербезопасности, и в целом государственная поддержка и консультирование частных компаний, работающих в этом направлении. Кроме того, планируется внедрение квантовой системы шифрования для защиты государственной тайны от утечек с использованием квантовых компьютеров, а также активное участие в разработке международных стандартов шифрования данных с целью продвижения собственных разработок в этой области на международном рынке.

5. Повышение эффективности работы национальной системы кибербезопасности. Признавая кибербезопасность неотъемлемой частью национальной безопасности, РК стремится совершенствовать организационные основы национальной системы кибербезопасности, состоящей из ряда государственных и частных органов. Для этого предлагается создать Национальный комитет кибербезопасности под контролем Управления национальной безопасности, а также принять Общий закон «О кибербезопасности», который будет регламентировать практические вопросы проведения специальных мероприятий по обеспечению кибербезопасности. Для реализации кризисного управления главенствующую роль предлагается передать НРС, ответственной за передачу информации о киберугрозах и работу со всеми государственными и частными организациями в кризисных ситуациях. С целью улучшить межведомственное взаимодействие и разработать стандартные процедуры и регламенты действий в условиях кибератак планируется подготовить Базовое руководство по кризисному управлению в области кибербезопасности. Наконец, в планах присутствует поддержка разных площадок сотрудничества и каналов обмена информацией между государственными органами и частными компаниями, вовлеченными в процесс обеспечения кибербезопасности государства, а также расширение программ подготовки специалистов в различных сферах, связанных с кибертехнологиями.

Таким образом, Стратегия кибербезопасности 2024 г. представляет собой достаточно политизированное видение вопросов и вызовов обеспечения национальной кибербезопасности, ставя во главу угла внешние факторы. Это отличает Стратегию от ее предыдущей редакции, выпущенной администрацией Мун Чжэ Ина в 2019 г., в которой не фигурирует Северная Корея как основной источник угроз кибербезо-

пасности, равно как и не акцентируется приоритет развития глобального сотрудничества. Также важным отличием является отсутствие цели создания единого координирующего органа, который выступит в роли «контрольной башни» всех организаций, связанных с обеспечением кибербезопасности. Если в Стратегии 2024 г. предполагается создать Национальный комитет кибербезопасности при Управлении национальной безопасности, одновременно увеличив полномочия НРС, то Стратегия 2019 г. видит сектор кибербезопасности государства как децентрализованную сеть государственных и частных организаций (вплоть до отдельных экспертов) и наделяет Управление национальной безопасности лишь общими функциями координации взаимодействия между ее участниками[13].

Международное сотрудничество Республики Корея в области кибербезопасности

США. Основным международным партнером в области кибербезопасности для РК является США. Сеул и Вашингтон — давние военные союзники, поддерживающие сотрудничество в области кибербезопасности на базе ряда форматов: Кибердиалог США — РК, рабочая группа по киберсотрудничеству США — РК, отдельная рабочая группа по противодействию северокорейским киберугрозам США — РК. Регулярные контакты поддерживаются также между американским Агентством по кибербезопасности и защите инфраструктуры и южнокорейскими НРС, Агентством интернет-безопасности и другими организациями.

На двустороннем саммите 26 апреля 2023 г., приуроченном к 70-летию военного альянса США и РК, лидеры двух государств Дж. Байден и Юн Сок Ёль провозгласили ряд инициатив по расширению сотрудничества по предотвращению киберугроз, защите критической инфраструктуры и борьбе с киберпреступлениями. Союзники договорились об учреждении Стратегической структуры сотрудничества в области кибербезопасности (U.S. — ROK Strategic Cybersecurity Cooperation Framework), подписав соответствующее соглашение в день саммита[14]. Предполагается, что РК и США совместно будут: разрабатывать и внедрять разнообразные инструменты по противодействию и сдерживанию угроз в киберпространстве; обмениваться информацией о злонамеренной киберактивности, включая кражу криптовалюты и незаконные финансовые операции; продвигать на международных площадках, в том числе в ООН, повестку, связанную с разработкой международно-правовых механизмов, мер укрепления доверия и норм поведения в киберпространстве. Помимо этого, важным направлением сотрудничества является совместная подготовка кадров, образовательная поддержка, обмены экспертами в области кибербезопасности, а также проведение военных учений. Первые совместные двусторонние учения под названием «Кибераль янс» были проведены 15–26 января 2024 г. В рамках этих учений на базе южнокорейского Командования кибероперациий специалисты из двух стран прошли подготовку по обмену информацией о хакерских атаках и реагированию на киберинциденты[15].

---

[13] National Cybersecurity Strategy. Seoul: National Security Office, 2019. P. 18.

[14] Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea // *The White House*. April 26, 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/leaders-joint-statement-in-commemoration-of-the-70th-anniversary-of-the-alliance-between-the-united-states-of-america-and-the-republic-of-korea/ (дата обращения: 15.12.2024).

[15] S. Korea, US hold 1st joint cyber security drill // *The Korea Times*. January 26, 2024. URL: https://www.koreatimes.co.kr/www/nation/2024/01/205_367685.html (дата обращения: 14.12.2024).

Также, во исполнение договоренностей от 26 апреля 2023 г., двумя месяцами позднее стороны учредили совместную рабочую группу по кибербезопасности. Предполагается, что этот орган займет роль основного канала взаимодействия представителей военных и разведывательных ведомств США и РК и ляжет в основу «информационного альянса» двух стран. На первом совещании рабочей группы, продлившемся три дня и завершившимся 22 июня 2023 г., обсуждались меры по противодействию краже криптовалютных активов[16]. Всего к настоящему моменту было проведено 7 заседаний рабочей группы, и основными темами обсуждений союзников в этом формате стали «противодействие незаконному получению доходов, хищению криптовалюты и кибершпионажу в оборонном секторе со стороны КНДР»[17]. Одним из результатов работы консультаций высокопоставленных представителей США и РК можно назвать разработку санкционных мер в отношении Северной Кореи. К примеру, в мае 2023 г. под ограничения Сеула и Вашингтона попали Пхеньянский университет автоматизации, Академия Кымсон, ряд подразделений Министерства обороны КНДР и ассоциированных с ним компаний, связанных, по мнению США и Южной Кореи, с подготовкой IT-специалистов и незаконными операциями с криптовалютой в интересах северокорейского руководства[18].

Треугольник США — РК — Япония. Наблюдаемая в последние годы тенденция к усилению военно-политического сближения США, Южной Кореи и Японии проявилась и в развитии сотрудничества в области кибербезопасности в рамках треугольника. 18 августа 2023 г. состоялся трехсторонний саммит в Кэмп-Дэвиде, обозначивший линию на интенсификацию военного сотрудничества между Сеулом, Вашингтоном и Токио, в том числе в целях совместного развития потенциала в области кибербезопасности и противодействия киберактивности КНДР[19]. Согласно кэмп-дэвидским договоренностям 7 декабря 2023 г. на базе внешнеполитических ведомств трех государств была учреждена рабочая группа по противодействию киберугрозам со стороны КНДР. Заседания рабочей группы проводятся ежеквартально, и к осени 2024 г. было проведено три раунда переговоров в данном формате. Основное взаимодействие в рамках рабочей группы сводится к обмену информацией о деятельности КНДР в киберпространстве и согласовании общей дипломатической линии по этому вопросу[20].

НАТО. Администрация Юн Сок Ёля прилагает значительные усилия для развития связей с блоком НАТО. В ноябре 2022 г. РК открыла свое представительство в НАТО, Юн Сок Ёль неоднократно посещал многосторонние саммиты блока и встречался с его официальными лицами, а в июле 2023 г. НАТО и РК приняли индивидуально адаптиро-

---

[16] *Choi Si-young*. S. Korea, US launch joint body on cybersecurity // *The Korea Herald*. June 23, 2023. URL: https://www.koreaherald.com/view.php?ud=20230623000533 (дата обращения: 14.12.2024).

[17] S. Korea, US stress commitment to disrupting NK revenue generation through cyber activities // *The Korea Times*. September 6, 2024. URL: https://www.koreatimes.co.kr/www/nation/2024/09/103_381985.html (дата обращения: 14.12.2024).

[18] 김동현, 김효정. 韓美, '北 사이버 외화벌이' 정조준…IT 업체·책임자 동시 제재(종합) [*Ким Дон Хён, Ким Хё Джон*. Южная Корея и США нацелены на «нелегальный зарубежный доход КНДР» в киберсфере: одновременные санкции в отношении IT-компаний и ответственных лиц] // 연합뉴스. 24.05.2023. URL: https://www.yna.co.kr/view/AKR20230523153551504?section=nk/news/all (дата обращения: 15.12.2024).

[19] The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States // *The White House*. August 18, 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/18/the-spirit-of-camp-david-joint-statement-of-japan-the-republic-of-korea-and-the-united-states/ (дата обращения: 15.12.2024).

[20] The 3rd Japan – U.S. – ROK Trilateral Diplomacy Working Group for Foreign Ministry Cooperation on North Korea's Cyber Threats // *Ministry of Foreign Affairs of Japan*. September 6, 2024. URL: https://www.mofa.go.jp/press/release/pressite_000001_00575.html (дата обращения: 15.12.2024).

ванную программу сотрудничества, включающую 11 направлений, в том числе сотрудничество в области кибербезопасности[21]. Южная Корея вместе с Японией, Новой Зеландией и Австралией является членом четверки «индо-тихоокеанских партнеров» (Indo-Pacific Four, IP4), которые представляют собой наиболее доверенных партнеров альянса на тихоокеанском пространстве. В перспективе сотрудничество по линии НАТО — IP4 может быть институционализировано и сфокусировано на таких сферах, как новые технологии и кибероборона[22].

В течение последних 4 лет РК принимает участие в международных учениях по кибербезопасности Locked Shields, проводимых под эгидой НАТО. На последних учениях в апреле 2024 г. Южную Корею представляли НРС, Министерство обороны, Министерство объединения и ряд подразделений из других государственных органов, а также частные организации[23]. В рамках учений специалисты из Южной Кореи прорабатывали вопросы борьбы с фейк-новостями, противодействия кибератакам на компьютерные сети средств спутниковой связи, объектов энергетики, промышленности, финансового сектора и др.[24]

Прочие партнеры. В последние годы РК также являлась участником многосторонних учений в области кибербезопасности. В мае 2024 г. Командование кибероперациий РК стало участником многосторонних учений Cyber Flag под эгидой США. В рамках учений представители 18 стран (в том числе члены разведывательного блока Five Eyes — Австралия, Новая Зеландия, Великобритания, США и Канада) ознакомились с регламентами реагирования на кибератаки, принятыми в вооруженных силах участников учений[25]. А в ноябре 2022 г. Южная Корея совместно с Малайзией выступила сопредседателем 9-й встречи подкомитета по кибербезопасности в рамках Совещания министров обороны АСЕАН+. В рамках данной работы состоялось симуляционное обучение по анализу вредоносного кода и криминалистическому анализу взломов ОС Windows, участниками учений стали представители стран АСЕАН, США, КНР, России, Японии, Новой Зеландии, Индии и Австралии[26].

Кроме того, можно выделить и установление партнерств с отдельными государствами. К примеру, в ноябре 2023 г. РК заключила с Великобританией декларацию о сотрудничестве в различных областях — т.н. Соглашение Даунинг-стрит, предусматривающее координацию усилий по противодействию и сдерживанию киберугроз в рамках «Стратегиче-

---

[21] 'Tailored partnership' with NATO to boost security cooperation // *Ministry of Foreign Affairs of ROK*. July 13, 2023. URL: https://overseas.mofa.go.kr/eng/brd/m_5674/view.do?seq=320840 (дата обращения: 15.12.2024).

[22] *Galic M.* (Ed.). Report of the Expert Study Group on NATO and Indo-Pacific Partners. Washington, DC: United States Institute of Peace, 2024. Pp. 20–22.

[23] *Kim Na-young*. S. Korea's spy agency set to join NATO-led cyber defense drill for 4th straight year // *Yonhap*. April 22, 2024. URL: https://en.yna.co.kr/view/AE№ 20240422005700320?section=national/defense (дата обращения: 15.12.2024).

[24] 배영경. 국정원, 나토 주관 사이버훈련 '락드쉴즈' 2년 연속 참여 [*Пэ Ён Гён*. Национальная разведывательная служба второй год подряд участвует в киберучениях НАТО Locked Shields] // 연합뉴스. 18.04.2022. URL: https://www.yna.co.kr/view/AKR20220418050200504?did=1195m (дата обращения: 15.12.2024).

[25] S. Korea to Join US-led Multinational Cyber Exercise // *KBS World*. May 5, 2024. URL: https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=185278 (дата обращения: 15.12.2024).

[26] 박수찬. 韓 주도 사이버훈련에 미·중·러 동시 참여 [*Пак Су Чхан*. США, Китай и Россия приняли участние в киберучениях, организованных Республикой Корея] // 세계일보. 16.11.2022. URL: https://www.segye.com/newsView/20221116516448?OutUrl=naver (дата обращения: 15.12.2024).

ского киберпартнерства Великобритания — РК»[27]. В июне 2024 г. Юн Сок Ёль провел переговоры с главой Узбекистана Ш. Мирзиёевым, договорившись в том числе о военном сотрудничестве по ряду направлений, включая повышение квалификации военнослужащих в области информационных технологий и кибербезопасности[28].

РК не только стремится устанавливать и развивать сотрудничество с разными партнерами, но и видит себя в качестве одного из мировых лидеров в области кибербезопасности. Как заявил Юн Сок Ёль на открытии международного форума Cyber Summit Korea в Сеуле в сентябре 2024 г.: «Южная Корея является центром кибербезопасности, постоянно развивающим свой оборонный потенциал в ответ на кибератаки со стороны враждебных сил, включая Северную Корею… мы закрепим свой международный статус в качестве центра подготовки специалистов в области кибербезопасности в Индо-Тихоокеанском регионе»[29].

Предварительные результаты и проблемы реализации политики администрации Юн Сок Ёля по обеспечению кибербезопасности

За последние несколько лет РК удалось продемонстрировать свои успехи в развитии кибербезопасности и укрепить позиции в международных рейтингах. К примеру, по данным Глобального индекса кибербезопасности (Global Cybersecurity Index, GCI) Международного союза электросвязи (International Telecommunication Union, ITU), в 2018 г. Южная Корея заняла 15-е место в мире и 5-е в АТР[30], а в 2020 г. поднялась уже на 4-ю позицию рейтинга, уступив лишь США, Великобритании, Саудовской Аравии (поделивших между собой вторую строчку) и Эстонии[31]. В последнем на данный момент рейтинге GCI, охватывающем период 2023–2024 гг., Южная Корея названа в числе мировых «ролевых моделей» обеспечения кибербезопасности. РК набрала максимальное количество баллов по всем индикаторам рейтинга и разделила первое место с 12 государствами мира (в том числе с Великобританией, Италией, Саудовской Аравией, Данией и др.), опередив таких игроков, как США, Сингапур, Япония и Австралия[32].

Тем не менее, за последние несколько лет в период президентства Юн Сок Ёля РК неоднократно становилась объектом хакерских атак. В октябре 2023 г. фишинговые рассылки массово получили сотрудники южнокорейских судостроительных компаний, в августе 2023 г. путем осуществления фишинговых атак на симуляционный центр была предпринята попытка нарушить ход совместных военных учений США и РК. Также в 2023 г. впервые кибератакам подверглись несколько правительственных органов РК, что привело к утере 175 млн вон. Известны и случаи массовых фишинговых рассылок по южнокорейским научно-исследовательским организациям (в частности – предприятиям

---

[27] The Downing Street Accord: A United Kingdom-Republic of Korea Global Strategic Partnership // *Government of United Kingdom.* November 2023. URL: https://assets.publishing.service.gov.uk/media/655e58f602e2e1000d433691/November_2023_-_The_Downing_Street_Accord__A_United_ Kingdom-Republic_of_Korea_Global_Strategic_Partnership.pdf (дата обращения: 15.12.2024).

[28] 박미영. 윤 "우즈벡에 한국산 고속철 수출…인프라 협력 모범 많이 만들것" [*Пак Ми Ён.* Юн Сок Ёль: «Строительство железной дороги в Узбекистане: мы создадим множество примеров инфраструктурного сотрудничества»] // 뉴시스. 14.06.2024. URL: https://www.newsis.com/view/?id=NISX20240614_0002773461 (дата обращения: 15.12.2024).

[29] 김승민. 윤 "한국, 북 사이버공격 방어해온 안보강국…인태 사이버훈련 허브될것" [*Ким Сын Мин*. Юн Сок Ёль: «Южная Корея — это центр безопасности, который защитил себя от атак Северной Кореи… она станет центром подготовки в облсти кибербезопасности в Индо-Пацифике»] // 뉴시스. 11.09.2024. URL: https://www.newsis.com/view/NISX20240911_0002884466 (дата обращения: 15.12.2024).

[30] Global Cybersecurity Index (CGI) 2018. Geneva: International Telecommunication Union, 2019. P. 58.

[31] Global Cybersecurity Index (CGI) 2020. Geneva: International Telecommunication Union, 2021. P. 25.

[32] Global Cybersecurity Index 2024: 5th Edition. Geneva: International Telecommunication Union, 2024. P. 24.

химической промышленности) от «фейковых» нанимателей[33]. Достаточно чувствительной для РК можно назвать серию кибератак на компании оборонного сектора в 2023–2024 гг. За этот период злоумышленникам удалось похитить свыше 250 файлов с информацией о технологиях лазерных и др. вооружений[34], заполучить техническую информацию по основному боевому танку К2, самолетам радиоэлектронной разведки проектов «Пэкту» и «Кымган»[35]. По результатам расследований, проводимых НРС, полицией и другими ведомствами РК (в том числе – совместно с ФБР США), ответственность за проведенные кибератаки южнокорейская сторона, как правило, возлагает на хакерские группировки Andariel и Lazarus, считая их связанными с Северной Кореей и отмечая, что некоторые из кибератак организованы напрямую из Пхеньяна с использованием арендованных серверов[36]. В числе других предполагаемых организаторов кибератак указываются и «хактивистские» группы из КНР[37]. Так или иначе, факты утечек информации, распространения вредоносного ПО и т.д. представляют весьма серьезный вызов для РК и демонстрируют, что на сегодняшний день защищенность государства от кибератак далеко не абсолютна, хотя факт принадлежности хакерских организаций Andariel и Lazarus к КНДР не является бесспорным и ставится под сомнение экспертами[38].

Что касается последних достижений политики кибербезопасности РК, то администрации Юн Сок Ёля на данный момент не удалось реализовать свою главную инициативу — создание Национального комитета кибербезопасности, предусмотренное проектом Общего закона «О кибербезопасности». Законопроект, представленный в ноябре 2022 г. по инициативе НРС, однако, за два года не был выдвинут на голосование и остается на стадии предварительного рассмотрения профильного парламентского комитета. Причина — «изменившаяся обстановка» в области кибербезопасности, а также стремление НРС внести в собственный законопроект правки[39], отражающие новый, «наступательный» (фактически — антисеверокорейский) вектор политики кибербезо-

---

[33] Significant Cyber Incidents // *Center for Strategic and International Studies.* 2024. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (дата обращения: 28.01.2025).

[34] 조문정. 北 해킹조직에 우리가 개발한 '드론 요격용 레이저포 기술' 통째로 털려 [*Чо Мун Джон*. Южнокорейская технология лазерного оружия для перехвата беспилотников полностью украдена Северной Кореей] // 뉴데일리. 05.12.2023. URL: https://www.newdaily.co.kr/site/data/html/2023/12/05/2023120500065.html (дата обращения: 28.01.2025).

[35] North Korean Cyberattacks: Theft of Sensitive Data on South Korea's Military Capabilities Including K2 Black Panther and SIGINT Aircraft // *Army Recognition.* August 14, 2024. URL: https://armyrecognition.com/news/army-news/army-news-2024/north-korean-cyberattacks-theft-of-sensitive-data-on-south-koreas-military-capabilities-including-k2-black-panther-and-sigint-aircraft (дата обращения: 28.01.2025).

[36] 조문정. 北 해킹조직에 우리가 개발한 '드론 요격용 레이저포 기술' 통째로 털려 [*Чо Мун Джон*. Южнокорейская технология лазерного оружия для перехвата беспилотников полностью украдена Северной Кореей] // 뉴데일리. 05.12.2023. URL: https://www.newdaily.co.kr/site/data/html/2023/12/05/2023120500065.html (дата обращения: 28.01.2025).

[37] Significant Cyber Incidents // *Center for Strategic and International Studies*. 2024. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (дата обращения: 28.01.2025).

[38] *Асмолов К.В*. Северокорейские хакеры: нестрашная правда // *РСМД.* 03.08.2018. URL: https://russiancouncil.ru/analytics-and-comments/analytics/severokoreyskie-khakery-nestrashnaya-pravda/ (дата обращения: 30.01.2025).

[39] 강진규. 국정원 '국가사이버안보법' 제정 본격화…연내 국회 제출 목표 [*Кан Чин Гю*. НРС инициировало принятие Общего закона «О кибербезопасности»: цель — представить проект в Национальную ассамблею до конца года] // 디지털투데이. 15.12.2024. URL: https://www.digitaltoday.co.kr/news/articleView.html?idxno=521388 (дата обращения: 15.12.2024).

пасности и соответствующие духу принятой в феврале 2024 г. Юн Сок Ёлем «проактивной» Стратегии кибербезопасности.

Еще большей проблемой является само содержание законопроекта, согласно которому главенствующая роль в реализации политики кибербезопасности отводится НРС. В законопроекте 2022 г. обозначены весьма размытые рамки ответственности за разработку и реализацию базового плана кибербезопасности, деятельность по предотвращению и реагированию на киберугрозы, оповещение о киберкризисах и др. Все эти задачи предполагается решать правительству РК, без четкого разграничения ответственности между НРС, Управлением национальной безопасности при правительстве РК и отдельными министерствами[40]. Как указывает в своем исследовании эксперт отдела киберрасследований Сеульского столичного полицейского управления Ким Ён Чжун, даже в случае принятия к рассмотрению в Национальной ассамблее Общего закона «О кибербезопасности» не удастся избежать разногласий, связанных с предоставлением больших полномочий НРС, следствием которых может стать нарушение прав человека и слежка за гражданскими лицами[41]. Вероятно, что законопроект может быть заблокирован оппозиционной Демократической партией «Тобуро», которая имеет парламентское большинство и в целом выступает за ограничение полномочий НРС (например, продвигая реформу по передаче от НРС к полиции полномочий по расследованию случаев шпионажа в интересах КНДР[42]). Таким образом, проект Общего закона «О кибербезопасности» рискует повторить судьбу Закона «О кибертерроризме», который так и остался на стадии законопроекта. Закон «О кибертерроризме» также подразумевал расширение сферы полномочий НРС, активно продвигался консервативной администрацией Пак Кын Хе в 2016 г. и встретил противодействие демократов[43]. Учитывая развернувшийся политический кризис в РК в декабре 2024 г., связанный с введением военного положения президентом Юн Сок Ёлем и последующими попытками оппозиции объявить импичмент президенту, перспективы принятия закона в его нынешнем виде минимальны.

В отсутствие успеха законодательных инициатив двумя президентскими указами в 2024 г. Юн Сок Ёль внес поправки в «Регулирование деятельности по обеспечению кибербезопасности». Данный документ, первая редакция которого вступила в силу в 2021 г., регламентирует основные вопросы, связанные с полномочиями и деятельностью в области кибербезопасности НРС и подотчетного ему Национального центра кибербезопасности. В двух поправках, принятых в 2024 г., предусматриваются: возможность создания экспертных комитетов при Национальном центре кибербезопасности; право директора НРС на отбор и назначение исследовательских организаций для выполнения работ по обеспечению кибербезопасности; право директора НРС инициировать расследование с целью доступа к цифровой информации и возможность ее добровольного предоставле-

[40] 김영준. 국가사이버안보 기본법 제정 방향 연구: 테러방지법과의 비교를 중심으로 [*Ким Ён Джун.* Анализ процесса принятия Общего закона «О кибербезопасности»: сравнение с Законом «О борьбе с терроризмом»] // 치안정책연구. 2024. Vol. 38. No. 1. 280–282쪽. DOI: 10.35147/knpsi.2024.38.1.267

[41] 김영준. 국가사이버안보 기본법 제정 방향 연구: 테러방지법과의 비교를 중심으로 [*Ким Ён Джун.* Анализ процесса принятия Общего закона «О кибербезопасности»: сравнение с Законом «О борьбе с терроризмом»] // 치안정책연구. 2024. Vol. 38. No. 1. 293–294쪽. DOI: 10.35147/knpsi.2024.38.1.267

[42] Main opposition slams ruling party's push to keep NIS' authority to conduct anti-communist investigations // *The Korea Times*. January 27, 2023. URL: https://www.koreatimes.co.kr/www/nation/2024/11/113_344360.html (дата обращения: 15.12.2024).

[43] *Park Woong-shin*. A Study on the Rationale of Cyberterrorism Prevention Act in ROK: Where Does the State's Obligation to Prevent Cyber Terror Originate? // *International Journal of Military Affairs*. 2016. No. 1(2). P. 20. DOI: 10.22471/militaryaffairs.2016.1.2.15

ния владельцем по запросу НРС; ответственность директора НРС за подготовку информации о киберугрозах, степени их влияния на национальную безопасность и возможных контрмерах, подготовленных по результатам анализа собранных НРС данных; возможность обращения НРС к другим государственным ведомствам с целью принятия мер по реагированию на киберугрозы в рамках их полномочий; возможность превентивного отслеживания, идентификации и нейтрализации деятельности хакерских организаций за рубежом и на территории КНДР; возможность создания государственно-частной платформы реагирования на киберугрозы под эгидой НРС и Управления национальной безопасности при президенте РК; полномочия НРС на введение систем защиты информации для государственных ведомств[44]. Поправки, таким образом, обеспечивают более широкие рамки для работы НРС в сравнении с редакцией «Регулирования деятельности по обеспечению кибербезопасности» 2021 г., а положение о возможности нейтрализации последствий деятельности хакерских организаций на территории КНДР, весьма характерно в свете принятия новой «проактивной» Стратегии кибербезопасности 2024 г.

Кроме этого, в целях выполнения приоритетных направлений деятельности, обозначенных в Стратегии кибербезопасности, в сентябре 2024 г. Управление национальной безопасности при президенте РК опубликовало «Основной план национальной кибербезопасности», в котором сформулированы задачи работы 14 министерств и других государственных органов. Всего в плане зафиксировано 100 задач, 33 из которых закреплены за НРС, 25 — за Министерством науки и ИКТ, 8 — за Национальным агентством полиции, 6 — за Министерством иностранных дел. Остальные ведомства имеют от 4 и менее закрепленных задач, также план предусматривает 7 коллективных задач, работу по которым предполагается скоординировано вести некоторым указанным в документе государственным органам. К ключевым коллективным задачам можно отнести предотвращение и противодействие киберпропаганде со стороны КНДР (ответственные — Национальное агентство полиции и Министерство объединения), подготовку экспертов в области военной кибербезопасности (Министерство обороны и Министерство науки и информационно-коммуникационных технологий), развитие национальной криптографической системы, в том числе с использованием квантово-устойчивых алгоритмов (НРС и Министерство науки и ИКТ)[45].

Наконец, среди объявленных в плане «120 задач государственной политики» инициатив также содержались мероприятия по подготовке кадров и создания резервных кибервойск. На данный момент, можно заключить, что за 2 года работы по этому направлению правительству Юн Сок Ёля не удалось добиться значительных успехов. Вооруженные силы и Министерство обороны РК прорабатывают детальные планы по включению офицеров и рядовых запаса с компетенциями в области кибероборонь в мобилизационный резерв по каждому подразделению ВС. Эта работа далека от завершения, и создание резервных кибервойск планируется не ранее 2025 г.[46] Также проект резервных кибервойск связывается и с процессом подготовки гражданских специалистов в универси-

[44] 사이버안보 업무규정 [Регулирование деятельности по обеспечению кибербезопасности] // 국가법령정보센터. URL: https://www.law.go.kr/lsInfoP.do?lsiSeq=261003&lsId=013942&chrClsCd=010202&urlMode=lsInfoP&viewCls=lsInfoP&efYd=20250101&v#0000 (дата обращения: 15.12.2024).

[45] 김경애. 국가안보실이 발표한 '국가 사이버안보 기본계획'… 어떤 내용 담겼나 [*Ким Кён Э*. Что входит в «Основной план национальной кибербезопасности», предложенный Управлением национальной безопасности?] // 보안뉴스. 02.09.2024. URL: https://m.boannews.com/html/detail.html?idx=132475 (дата обращения: 15.12.2024).

[46] 김귀근. '사이버 예비군' 2년 뒤 창설한다…전시 사이버작전 담당 [*Ким Кви Гын*. Резервные кибервойска будут созданы через 2 года и будут отвечать за проведение кибероперaций в условиях военного времени] // 연합뉴스. 03.10.2023. URL: https://www.yna.co.kr/view/AKR20230926152900504 (дата обращения: 15.12.2024).

тетах, отобранных Министерством науки и ИКТ, с последующим планом предоставления им офицерских позиций. Подготовка киберспециалистов тесно связана с национальной образовательной программой «100 тысяч киберталантов», опыт реализации которой за последние три года продемонстрировал весьма скромные успехи. По данным, предоставленным Агентством интернет-безопасности РК, бюджет программы на 2025 г. был сокращен на 10 % в сравнении с предыдущим годом (с 24 млрд вон в 2024 г. до 22 млрд в 2025 г.). Снизилось общее число специалистов, прошедших через подготовку (15 600 чел. в 2023 г. и около 10 000 за период январь — август 2024 г.), причем особенно сильно сократилось количество выпускников программы в регионах РК за пределами Сеула (1 600 в 2024 г. против 6 000 в 2023 г.)[47].

* * *

Годы президентства Юн Сок Ёля ознаменовались развитием «проактивной» политики Республики Корея по обеспечению кибербезопасности. В ее основе лежит развитие наступательного киберпотенциала и жесткое противодействие киберугрозам со стороны КНДР, предусматривающее в том числе превентивное отслеживание, идентификацию и нейтрализацию деятельности хакерских организаций, находящихся на территории Северной Кореи. Также «проактивный» вектор предполагает и укрепление международного сотрудничества — за последние три года Юн Сок Ёль весьма успешно активизировал контакты с многими странами мира, результатом чего стало расширение участия Южной Кореи в международных учениях по кибербезопасности по линии НАТО, АСЕАН, альянса США — РК и т.д.

Политика Юн Сок Ёля также направлена на централизацию процесса управления частными и государственными организациями в сфере кибербезопасности, расширение полномочий НРС по координации работы всех релевантных ведомств и сбору необходимых данных. Цель этой политики — создание своеобразного дуумвирата НРС и Управления национальной безопасности при президенте РК. На базе Управления национальной безопасности предполагается создать Национальный комитет кибербезопасности, который выступит в роли «контрольной башни» и будет заниматься продвижением общей политики кибербезопасности в гражданском и военном секторах, курировать развитие передовых технологий. Для НРС отводится при этом более практическая роль, связанная с экспертизой систем безопасности, сбором данных и координацией работы государственных органов при реагировании на киберкризисы, вызванные хакерскими атаками и т.д.

Стоит отметить, что данный вектор политики развивается в условиях общественной дискуссии. Комментируя ситуацию, сложившуюся после объявления военного положения в РК в ночь со 2 на 3 декабря 2024 г., в своем выступлении президент Юн Сок Ёль упомянул отказ Национальной избирательной комиссии допустить НРС к проверке систем безопасности. По словам президента, в условиях интенсификации хакерских атак со стороны КНДР информационная безопасность государственных органов Южной Кореи должна быть укреплена во избежание утечек информации[48]. Оппозиция широко критикует этот подход, считая, что северокорейская угроза намеренно преувеличена президентом с целью оправдать расширение полномочий НРС, что является злоупотреблением вла-

[47] 김영명. 2022~2024년 사이버보안 10만 인재 양성, 예산 삭감 등으로 인재 배출 실적 부진 [*Ким Ён Мён*. Программа «100 тысяч киберталантов» продемонстрировала плохие показатели в 2022–2024 гг. по причине сокращения бюджета и др.] // 보안뉴스. 02.10.2024. URL: https://m.boannews.com/html/detail.html?idx=133297 (дата обращения: 15.12.2024).

[48] Full text of South Korean President Yoon Suk Yeol's address to the nation on Thursday // *The Korea Herald*. December 12, 2024. URL: https://news.koreaherald.com/view.php?ud=20241212050073 (дата обращения: 15.12.2024).

стью и ведет к нарушениям прав человека[49]. Как результат, Юн Сок Ёлю не удалось реализовать главную инициативу своей политики и принять Общий закон «О кибербезопасности», предусматривающий создание Национального комитета кибербезопасности. В условиях внутриполитического кризиса, развивающегося после объявления военного положения в декабре 2024 г., шансы на завершение этой реформы можно оценить как минимальные. Данная ситуация практически идентична попыткам администрации Пак Кын Хе принять Закон «О кибертерроризме», также подразумевавший расширение сферы полномочий НРС и заблокированный оппозиционной фракцией. В свете возможной смены президентской администрации в РК в 2025 г. следует ожидать, что основные инициативы Юн Сок Ёля в области централизации сектора кибербезопасности могут быть свернуты полностью (в случае прихода к власти оппозиционной демократической администрации) либо переосмыслены в новом виде (при условии сохранения власти консерваторами). Антисеверокорейская направленность и «наступательный» характер Стратегии кибербезопасности 2024 г., вероятно, также будут, как минимум, смягчены в риторике и официальных документах следующей президентской администрации – однако, во многом это будет зависеть от обстановки на Корейском полуострове и особенностей отношений Севера и Юга в будущие годы. Что касается результатов политики кибербезопасности Юн Сок Ёля, которые сохранятся в качестве задела для будущей власти в РК – к таковым можно отнести серьезно расширившуюся сеть международных партнерств, наработанные компетенции по защите информации и реагировании на киберугрозы, достигнутый прогресс по созданию киберрезеров в ВС РК. Все это, вероятно, станет значимым подспорьем для продолжения и расширения подготовки южнокорейских специалистов в области кибербезопасности в ближайшие годы.

Литература

Асмолов К.В. Северокорейские хакеры: нестрашная правда // *РСМД*. 03.08.2018. URL: https://russiancouncil.ru/analytics-and-comments/analytics/severokoreyskie-khakery-nestrashnaya-pravda/ (дата обращения: 30.01.2025).

Волощак В.И. Проблемы развития национальной системы кибербезопасности Республики Корея // *Проблемы Дальнего Востока*. 2018. № 3. С. 117–125.

Full text of South Korean President Yoon Suk Yeol's address to the nation on Thursday // *The Korea Herald*. December 12, 2024. URL: https://news.koreaherald.com/view.php?ud=20241212050073 (дата обращения: 15.12.2024).

Galic M. (Ed.). Report of the Expert Study Group on NATO and Indo-Pacific Partners. Washington, DC: United States Institute of Peace, 2024. 64 p.

Global Cybersecurity Index (CGI) 2018. Geneva: International Telecommunication Union, 2019. 92 p.

Global Cybersecurity Index (CGI) 2020. Geneva: International Telecommunication Union, 2021. 172 p.

Global Cybersecurity Index 2024: 5th Edition. Geneva: International Telecommunication Union, 2024. 151 p.

Jeong Yeonoh, Choi Jin-Young, Park Seunghyun. Improvement of the Defense Planning and Management System to Implement the ROK's National Cybersecurity Strategy // *The Korean Journal of Defense Analysis*. 2023. Vol. 35. No. 3. Pp. 337–360.

Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea // *The White House*. April 26, 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/leaders-joint-statement-in-commemoration-of-the-70th-anniversary-of-the-alliance-between-the-united-states-of-america-and-the-republic-of-korea/ (дата обращения: 15.12.2024).

National Cybersecurity Strategy. Seoul: National Security Office, 2019. 27 p.

[49] "대공수사권 복원" 야만의 시대로 회귀하겠다는 것 [Восстановление права НРС на проведение контрразведывательных расследований — возврат в варварскую эпоху] // 참여연대. 07.03.2024. URL: https://www.peoplepower21.org/government/1960157?ckattempt=2 (дата обращения: 15.12.2024).

Park Woong-shin. A Study on the Rationale of Cyberterrorism Prevention Act in ROK: Where Does the State's Obligation to Prevent Cyber Terror Originate? // *International Journal of Military Affairs*. 2016. No. 1(2). Pp. 15–20. DOI: 10.22471/militaryaffairs.2016.1.2.15

The Downing Street Accord: A United Kingdom-Republic of Korea Global Strategic Partnership // *Government of United Kingdom*. November, 2023. URL: https://assets.publishing.service.gov.uk/media/655e58f602e2e1000d433691/November_2023_-_The_Downing_Street_Accord__A_United_Kingdom-Republic_of_Korea_Global_Strategic_Partnership.pdf (дата обращения: 15.12.2024).

The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States // *The White House*. August 18, 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/18/the-spirit-of-camp-david-joint-statement-of-japan-the-republic-of-korea-and-the-united-states/ (дата обращения: 15.12.2024).

국가 사이버안보 전략 [Национальная стратегия кибербезопасности]. 서울: 대통령실 국가안보실, 2024. 35쪽.

김영준. 국가사이버안보 기본법 제정 방향 연구: 테러방지법과의 비교를 중심으로 [*Ким Ён Джун*. Анализ процесса принятия Общего закона «О кибербезопасности»: сравнение с Законом «О борьбе с терроризмом»] // 치안정책연구. 2024. Vol. 38. No. 1. 267–300쪽. DOI: 10.35147/knpsi.2024.38.1.267

사이버안보 업무규정 [Регулирование деятельности по обеспечению кибербезопасности] // 국가법령정보센터. URL: https://www.law.go.kr/lsInfoP.do?lsiSeq=261003&lsId=013942&chrClsCd=010202&urlMode=lsInfoP&viewCls=lsInfoP&efYd=20250101&v#0000 (дата обращения: 15.12.2024).

윤석열 정부 120대 국정 과제 [120 задач государственной политики правительства Юн Сок Ёля]. 서울: 대한민국정부, 2022. 197쪽.

Republic of Korea's Cybersecurity Policy: Objectives, Instruments, International Cooperation

Valentin I. Voloshchak

Ph.D. (History), Researcher, Laboratory of Asia-Pacific Studies, Institute of History, Archaeology and Ethnology, Far-Eastern Branch of the Russian Academy of Sciences (address: 89, Pushkinskaya Str., Primorsky Krai, Vladivostok, 690001, Russia). ORCID: 0000–0001–7557–7494. E-mail: v.voloshchak@ihaefe.ru

Received 16.12.2024.

Abstract:

The article is devoted to the analysis of the main directions of the Republic of Korea's cybersecurity policy after the Yoon Suk Yeol administration came to power in 2022. Drawing from the analysis of ROK's official documents, including the new 2024 Cybersecurity Strategy, the author demonstrates that the main aspect of Yoon Suk Yeol's "proactive" cybersecurity policy is an appeal to the factor of the North Korean cyber threat, which necessitates the development of offensive cyber potential and preventive response to cyber threats. The author also notes that over the past three years, South Korea has expanded its participation in international cybersecurity exercises (including under the auspices of NATO) and, in general, strengthened cooperation in the field of cybersecurity with many foreign partners. Finally, an important part of the cybersecurity policy is the reform of public and private cybersecurity sector organizations' activities management, aimed at increasing the role of the National Intelligence Service and the creation of a single coordinating body — the so-called National Cyber Security Committee. The author concludes that in the face of opposition that disagrees with the centralization policy and believes that strengthening the role of the National Intelligence Service in ensuring national cybersecurity is an abuse of power and leads to human rights violations, Yoon Suk Yeol failed to implement the main initiative of his cybersecurity policy and pass the Framework Act on Cybersecurity. At the same time, this situation is almost identical to the Park Geun Hye administration's attempts to pass the Cyberterrorism Act, which also implied an expansion of the scope of National Intelligence Service authority and was subsequently blocked by the opposition faction.

Key words:

Cybersecurity, Republic of Korea, strategy, intelligence, centralization, cyber threats, reform.

Funding sources:

The article is prepared under a federal assignment No. 1023110200001–7–5.6.1 “The Asia-Pacific region in the context of rivalry between the West and the Greater East for the formation of a new world order”.

For citation:

Voloshchak V.I. Republic of Korea's Cybersecurity Policy: Objectives, Instruments, International Cooperation // Far Eastern Studies. 2025. No. 1. Pp. 7–22. DOI: 10.31857/S0131281225010016.

References

Asmolov K.V. Severokorejskie hakery: nestrashnaya pravda [North Korean Hackers: Not the Scary Truth]. *RSMD.* 03.08.2018. URL: https://russiancouncil.ru/analytics-and-comments/analytics/severokoreyskie-khakery-nestrashnaya-pravda/ (accessed: 30.01.2025). (In Russ.)

Full text of South Korean President Yoon Suk Yeol's address to the nation on Thursday. *The Korea Herald*. December 12, 2024. URL: https://news.koreaherald.com/view.php?ud=20241212050073 (accessed: 15.12.2024).

Galic M. (Ed.). Report of the Expert Study Group on NATO and Indo-Pacific Partners. Washington, DC: United States Institute of Peace, 2024. 64 p.

Global Cybersecurity Index (CGI) 2018. Geneva: International Telecommunication Union, 2019. 92 p.

Global Cybersecurity Index (CGI) 2020. Geneva: International Telecommunication Union, 2021. 172 p.

Global Cybersecurity Index 2024: 5th Edition. Geneva: International Telecommunication Union, 2024. 151 p.

Jeong Yeonoh, Choi Jin-Young, Park Seunghyun. Improvement of the Defense Planning and Management System to Implement the ROK’s National Cybersecurity Strategy. *The Korean Journal of Defense Analysis*. 2023. Vol. 35. No. 3. Pp. 337–360.

Leaders’ Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea. *The White House*. April 26, 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/leaders-joint-statement-in-commemoration-of-the-70th-anniversary-of-the-alliance-between-the-united-states-of-america-and-the-republic-of-korea/ (accessed: 15.12.2024).

National Cybersecurity Strategy. Seoul: National Security Office, 2019. 27 p.

Park Woong-shin. A Study on the Rationale of Cyberterrorism Prevention Act in ROK: Where Does the State's Obligation to Prevent Cyber Terror Originate? *International Journal of Military Affairs*. 2016. No. 1(2). Pp. 15–20. DOI: 10.22471/militaryaffairs.2016.1.2.15

The Downing Street Accord: A United Kingdom-Republic of Korea Global Strategic Partnership. *Government of United Kingdom*. November, 2023. URL: https://assets.publishing.service.gov.uk/media/655e58f602e2e1000d433691/November_2023_-_The_Downing_Street_Accord__A_United_Kingdom-Republic_of_Korea_Global_Strategic_Partnership.pdf (accessed: 15.12.2024).

The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States. *The White House*. August 18, 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/18/the-spirit-of-camp-david-joint-statement-of-japan-the-republic-of-korea-and-the-united-states/ (accessed: 15.12.2024).

Voloshchak V.I. Problemy razvitiya nacional'noj sistemy kiberbezopasnosti v Respublike Koreya [The Problems of National Cyber Security System Development in Republic of Korea]. *Problemy Dal’nego Vostoka*. 2018. No. 3. S. 117–125. (In Russ.)

국가 사이버안보 전략 [National Cybersecurity Strategy]. 서울: 대통령실 국가안보실, 2024. 35쪽. (In Kor.)

김영준. 국가사이버안보 기본법 제정 방향 연구: 테러방지법과의 비교를 중심으로 [*Kim Young-Jun.* Study on the direction of enactment of the National Cyber Security Framework Law: Focusing on comparison with the Anti-Terrorism Act]. 치안정책연구. 2024. Vol. 38. No. 1. 267–300쪽. DOI: 10.35147/knpsi.2024.38.1.267. (In Kor.)

사이버안보 업무규정 [Regulations on Cybersecurity Services]. 국가법령정보센터. URL: https://www.law.go.kr/lsInfoP.do?lsiSeq=261003&lsId=013942&chrClsCd=010202&urlMode=lsInfoP&viewCls=lsInfoP&efYd=20250101&v#0000 (accessed: 15.12.2024). (In Kor.)

윤석열 정부 120대 국정 과제 [Yoon Seok-yeol's government's 120 National Tasks]. 서울: 대한민국정부, 2022. 197쪽. (In Kor.)