Д. Трамп склонен придерживаться идеи **America First** и действовать в рамках сугубо меритократических установок, что предопределяет уход от демократической атрибутики и пренебрежение некоторыми ценностями и интересами государств-партнеров в рамках реализации внешнеполитического курса США.

Обзор имеющих отношение к международной проблематике инициатив действующего президента США объективирует некоторые тренды относительно структурного реформирования современной системы международных отношений и категоризирует существующие в глобальной плоскости проблемы. При этом основным условием гармонизации интересов в рамках мирового политического процесса является формулирование обновленных ценностей и инструментария, приемлемых для большинства глобальных политических игроков.

Источники и литература:

1. Henry Kissinger: 'We Are In A Very, Very Grave Period' [Electronic resource] // The Financial Times. – 2018. – Mode of access: https://www.ft.com/content/926a66b0-8b49-11e8-bf9e-8771d5404543. – Date of access: 16.02.2020.

2. Transcript: Donald Trump Expounds On His Foreign Policy Views [Electronic resource] // The New York Times. – 2016. – 27 March. – Mode of access: https://www.nytimes.com/2016/03/27/us/politics/donald-trump-transcript.html. – Date of access: 16.02.2020.

СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ ФРГ: ОТВЕТ НА ГЛОБАЛЬНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ НАЧАЛА XXI в.

Т.Г. Хришкевич (Псков)

Информационные технологии (ИТ) являются двигателем современного глобального информационного общества. Одновременно с ростом значения интернета растёт осознание недостаточной надежности ИТ-систем, серверов и сетевых компонентов. Рост угроз гражданам, организациям, государствам, международному сообществу становится постоянным явлением. Экономический, социальный ущерб всё больше соседствуют с проблемой международной безопасности и угрозой терроризма, создавая дисбаланс между нападением и защитой.

В настоящее время, проблемы кибербезопасности весьма разносторонни и нельзя недооценивать каждую из них. Одна из основных заключается в том, что в используемом программном обеспечении (ПО) слишком много уязвимостей. По данным немецкого Института информационных технологий и факультета Потсдамского университета (Институт Хассо Платтнера, Hasso-Plattner-Institut für Digital Engineering), за период с 2011 по 2018 гг. количество уязвимостей в ПО выросло с 4383 до 11003 в год [12, s. 3]. Атаки

на информационную инфраструктуру становятся все более сложными, наблюдается растущая профессионализация хакеров. Масштабы киберпространства позволяют проводить завуалированные атаки, злоупотребляя уязвимыми системами жертв в качестве инструмента. Преступники, террористы используют киберпространство в качестве поля для своих действий. Опасность представляют не только мошеннические схемы, но и угрозы энергетике, военной сфере. От целенаправленных или даже случайных сбоев в равной степени страдают государство, экономика и общество. Таким образом, информационная безопасность становится всё более важной повесткой для правительств и разработчиков антивирусного ПО.

В Федеративной Республике Германия в 2010-е гг. подобные атаки стали повседневным явлением. Например, в мае 2015 г. взломщики проникли во внутреннюю компьютерную сеть бундестага, летом 2018 г. немецкие спецслужбы пресекли широкую атаку на энергосети. Рост атак и их интернационализация привели 29 августа 2018 г. к решению о создании в ФРГ Агентства по инновациям в области кибербезопасности. Оно приступило к работе в начале 2019 г. На финансирование проекта было выделено 200 млн. евро до 2022 г. Приоритетными проектами агентства, по словам министра обороны У. фон дер Ляйен, должны были стать поддержка собственных технологий шифрования и развитие ПО [2].

За обеспечением кибербезопасности в стране наблюдает ряд структур, например, ведомство по охране конституции, созданное в 1990 г. Так, например, отчет ведомства за 2018 г. особое внимание уделяет опасности, исходящей от многочисленных разведывательных служб: «Шпионаж через кибератаки стал стандартным инструментом с высоким потенциалом для их возможных и фактических жертв. Кибератаки открывают эффективные возможности для получения ценной информации в цифровом виде со сравнительно низким риском». Причем, акценты, расставляемые ведомством, нельзя назвать лишенными политической конъюнктуры, особенно в отношении России: «С охлаждением политических отношений России со многими западными государствами разведывательный сбор информации приобрел важное значение. В центре внимания России – политика, экономика, наука и техника, а также военные. Информационная потребность при этом широка и ориентирована на текущие события и события в зависимости от политической ситуации, но прежде всего на такие цели, которые касаются российских интересов. В Германии также активно работают российские разведывательные службы с высокими организационными, кадровыми и финансовыми затратами. Особый интерес представляют возможные переговорные позиции Германии и Запада или вопрос о том, какие контрмеры следует ожидать в политическом или экономическом отношении. Основными направлениями являются российско-германские отношения, а также политика союзников Германии в НАТО и ЕС, не в последнюю

очередь из-за событий на Украине и в сирийском конфликте. В частности, вопрос об отмене санкций, введенных ЕС в 2014 году» [13, s. 286].

В отношении Китая также сделаны обширные допущения: «В июле 2017 г. Китайский народный конгресс принял закон «О национальной разведке», благодаря этому органы безопасности теперь имеют многочисленные формально кодифицированные специальные права на разведывательную деятельность в стране и за рубежом практически без ограничений» [13, s. 296]. Кроме политических выводов, ведомство по охране конституции публикует регулярные многостраничные «Cyber-Brief». Это рекомендации по кибербезопасности, а также сводные данные ip-адресов и вредоносных сайтов, откуда были совершены кибер-атаки [7].

Вся совокупность федеральных структур, сосредоточенных на цифровой защите, базируется на Стратегии кибербезопасности (Cyber-Sicherheitsstrategie für Deutschland), которая была принята федеральным правительством в феврале 2011 г. [9]. В ней ставилась цель укрепить международное сотрудничество по созданию глобальной кибербезопасности. В рамках этой стратегии федеральное правительство усилило разработку соответствующих практических мер доверия и безопасности. Обеспечение кибербезопасности называлось центральной проблемой для государства, экономики и общества в национальном и международном контексте, что требовало соблюдения международных правил поведения и стандартов: «Только сочетание внутриполитических и внешнеполитических мер может позволить решить проблему». Стратегия подчеркивала необходимость сотрудничества в рамках Организации Объединенных Наций, ЕС, Совета Европы, НАТО, G8, ОБСЕ и других транснациональных организаций.

Стратегия 2011 г. состояла из 10 разделов, большая часть из которых была посвящена внутренней безопасности: защите важнейших информационных инфраструктур, укреплению ИТ-безопасности в государственном управлении, создание национального Центра кибер-обороны, расширению кадрового потенциала и борьбе с преступлениями в кибер-пространстве. В тоже время раздел 7 был посвящен взаимодействию в целях обеспечения кибербезопасности в Европе и мире. Стратегия декларировала поддержку расширения мандата Европейского агентства по сетевой и информационной безопасности (ENISA) в отношении угроз в области информационных технологий, а также объединение ИТ-юрисдикций в учреждениях ЕС. Особое внимание было уделено целенаправленной координации действий ООН, ОБСЕ, Совета Европы, ОЭСР и НАТО. Северо-Атлантический альянс стратегия называла основой трансатлантической безопасности: «Мы выступаем за приверженность альянсу, единым стандартам безопасности, которые государства-члены могут добровольно взять на себя, как это предусмотрено в новой стратегической концепции НАТО» [9, s. 11].

В 2016 г. Стратегия безопасности была модернизирована в соответствии с изменившимися условиями. Она называла четыре основных

«поля действия» руководящих принципов, три из которых в основном затрагивали внутреннюю безопасность: цифровая среда, государство и экономика, архитектура кибербезопасности. Четвертое поле было посвящено необходимости более активного позиционирования Германии на европейском и международном уровнях [10]. Стратегия делала упор на стремлении к укреплению двусторонней и региональной поддержки в области развития и расширения кибер-возможностей международных правоохранительных органов. Инструментами такой политики должны оставаться: Северо-Атлантический альянс, как «краеугольный камень безопасности Германии, а также евроатлантической безопасности», международные стабилизационные операции, сдерживание и оборона в контексте гибридных угроз, разработка собственных стратегий кибербезопасности, принятие новых законодательных актов, создание учреждений, научные исследования, мероприятия по обучению и повышению квалификации персонала, а также региональные инициативы.

В целях более эффективной кибер-защиты в государстве появился ряд дополнительных федеральных структур, в частности, в рамках Министерства внутренних дел было создано Федеральное ведомство по информационной безопасности, в котором появился специальный Центр кибербезопасности (Кибер-Абверцентр, Cyber-AZ). Он был призван оптимизировать оперативное сотрудничество и координировать меры защиты. Его целью стало противодействие таким угрозам как кибер-шпионаж, кибертерроризм и киберпреступность, а методами оптимизация оперативного сотрудничества государственных органов, обмен информацией, быстрые оценки и полученные из них конкретные рекомендации действия [8].

Особый интерес в изучении теории и практики обеспечения кибербезопасности в ФРГ представляют ежегодные отчеты федерального правительства о состоянии усилий по контролю над вооружениями, разоружению и нераспространению, а также развитию потенциала вооруженных сил. С 2012 г., в соответствии с целями, поставленными в стратегии кибербезопасности 2011 г., отчеты фиксируют мероприятия, направленные на обеспечение кибербезопасности внутри страны и за ее пределами. Среди них участие в работе правительственной экспертной группы ООН по кибербезопасности и рабочей группы ОБСЕ по разработке мер в целях обеспечения доверия и безопасности в киберпространстве, а также саммитах G8; мероприятия по защите прав человека в киберпространстве в постоянном представительстве Германии при ООН; проведение конференций и симпозиумов в Берлине на тему «Сохранение свободы и стабильности кибер-пространства»; проведение межведомственных двусторонних кибер-консультаций с Китаем, Индией, Южной Кореей и Израилем; обмен информацией с США и партнерами по ЕС (Францией и Великобританией) и многое другое [3–6].

Особое место информационная безопасность заняла в борьбе терроризмом. Её совершенствование привело к созданию базы данных по борьбе с терроризмом (Anti-Terror-Datei, ATD). Предполагалось, что целый ряд ведомств

сможет получить доступ к конфиденциальной информации. В их ряду стояли Федеральная криминальная полиция, Федеральное ведомство по охране конституции, Федеральная разведывательная служба, таможня. В то же время информационная прозрачность вызвала неоднозначную реакцию. База данных была воспринята как способ тотального контроля над гражданами. В защиту ATD перед Федеральным конституционным судом выступил министр внутренних дел Германии Ханс-Петер Фридрих: «ATD это инструмент, который имеет большое значение в борьбе с международным терроризмом» [11].

Подводя итог, следует сказать, что обеспечение кибербезопасности в настоящее время является одним из самых актуальных и востребованных направлений деятельности служб безопасности не только в ФРГ, но и в других странах, являющихся ключевыми игроками мировой политики. Многочисленные атаки на демократические институты, международные организации, инфраструктуру и жизненно важные промышленные объекты приводят как к техническому ущербу, так и репутационному. Они подрывают доверие общества, доверие между странами, политическими и экономическими системами. Таким образом, учитывая высочайшую степень взаимозависимости государств в глобальном пространстве, важнейшей политической задачей, к которой стремится современная Германия в обеспечении кибербезопасности становятся: внутренняя устойчивость; устойчивость отношений между странами-партнерами; сдерживание угроз; правовое регулирование, включая международный уровень; обмен передовым опытом.

Источники и литература:

1. Anti-Terror-Datei (ATD) [Elektronische Ressource]. – Zugriffsart: https://www.verfassungsschutz.de/de/service/glossar/anti-terror-datei-atd. – Behandlungsdatum: 31.03.2020.

2. Ausländische Hacker dringen in deutsches Regierungsnetzein. 28.02.2018 [Elektronische Ressource]. – Zugriffsart: https://www.welt.de/wirtschaft/article174062118/Datensicherheit-Auslaendische-Hacker-dringen-in-deutsches-Regierungsnetz-ein.html. – Behandlungsdatum: 31.03.2020.

3. Bericht der Bundesregierungzum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitungsowieüber die Entwicklung der Streitkräftepotenziale. Jahresabrüstungsbericht 2012. –Berlin : H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, 2012. – 237 s.

4. Bericht der Bundesregierungzum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitungsowieüber die Entwicklung der Streitkräftepotenziale. Jahresabrüstungsbericht 2013. – Berlin : H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, 2013.– 264 s.

5. Bericht der Bundesregierungzum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitungsowieüber die Entwicklung der Streitkräftepotenziale 2014. – Berlin : H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, 2014.– 154 s.

6. Bericht der Bundesregierungzum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitungsowieüber die Entwicklung der Streitkräftepotenziale 2014. – Berlin : H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, 2015. – 159 s.

7. BfV Cyber-Brief. Nr. 02/2017. Hinweis auf aktuelleAngriffskampagne. – Köln : Bundesamt für Verfassungsschutz, 2017.– 15 s.

8. Cyber-Abwehrzentrum [Elektronische Ressource]. – Zugriffsart: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html. – Behandlungsdatum: 31.03.2020.

9. Cyber-Sicherheitsstrategie für Deutschland 2011. – Berlin : Silber DruckoHG, Niestetal, 2011. – 20 s.

10. Cyber-Sicherheitsstrategiefür Deutschland 2016. – Berlin : Bonifatius GmbH, Druck – Buch – Verlag, 2016. – 25 s.

11. Karlsruhe sieht «rechtliche Probleme» [Elektronische Ressource]. – Zugriffsart: http://www.focus.de/politik/deutschland/tid-28016/anti-terror-datei-vor-dem-bundesverfassungsgericht-karlsruhe-sieht-rechtliche-probleme_aid_854472.html. – Behandlungsdatum: 30.03.2020.

12. Pohlmann, N. Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. – Wiesbaden : Springer Fachmedien Wiesbaden GmbH, einTeil von Springer Nature, 2019. – 611 s.

13. Verfassungsschutzbericht 2018. – Berlin : Kern GmbH, Bexbach, 2018. –388 s.

ГЕРМАНИЯ НА 40-Й СЕССИИ ГЕНЕРАЛЬНОЙ КОНФЕРЕНЦИИ ЮНЕСКО

С.Ф. Свилас, Ю.В. Станкевич (Минск)

Глобализации с ее трансграничными вызовами делает международное сотрудничество в духовной сфере особенно актуальным. Результаты 40-й сессии Генеральной конференции ЮНЕСКО, проходившей в Париже с 12 по 27 ноября 2019 года, свидетельствуют о том, что Организации предстоит стать лидером в мобилизации международных усилий в области образования, науки, культуры, инноваций и новых технологий. Помимо делегаций государств-членов Организации и ассоциированных членов (193), в работу сессии были активно вовлечены межправительственные и неправительственные организации [2].

Одним из приоритетных вопросов, обсуждавшихся на 40-й сессии, по-прежнему оставалось образование. На ЮНЕСКО как специализированное учреждение системы ООН возложена ответственность за координацию действий международного сообщества для достижения Цели 4 в области устойчивого развития (ЦУР 4) – качественное образование для всех, важнейшим аспектом которого является поддерживаемая Германией стратегия по распространению грамотности среди молодежи и взрослых. Сессия утвердила Рекомендацию по созданию открытых лицензионных образовательных ресурсов. Лицензия обеспечит свободный доступ, а также бесплатное пользование, редактирование и распространение материалов без каких-либо ограничений. Авторы материалов будут сами определять, какие права пользования они предоставят, а какие оставят за собой.