Санкт-Петербургский государственный университет

**КИНАШ Екатерина Игоревна**

Выпускная квалификационная работа

**Сотрудничество ЕС и НАТО в сфере кибербезопасности: особенности подходов иперспективы развития**

**EU-NATO cooperation in the field of cybersecurity: features of approaches and development prospects**

Уровень образования: Магистратура

Направление 41.04.05 «Международные отношения»

Основная образовательная программа

ВМ.5558.2020 «Европейские исследования»

**Научный руководитель:**

доцент кафедры европейских исследований

факультета международных отношений СПбГУ, к.и.н.

Заславская Наталья Генриховна

**Рецензент:**

старший преподаватель Высшей школы международных отношений

Гуманитарного института СПбПУ, к.полит.н.

Вовенда Алексей Викторович

Санкт-Петербург

2022

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** 3](#_Toc103556701)

[**ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ СОТРУДНИЧЕСТВА НАТО И ЕС В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ** 14](#_Toc103556702)

[1.1. Политика кибербезопасности как объект научного анализа 14](#_Toc103556703)

[1.2. Подходы к изучению взаимодействия НАТО и ЕС по вопросам кибербезопасности 21](#_Toc103556704)

[**ГЛАВА 2. ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ В СТРАТЕГИЯХ ЕС И НАТО: ОБЩИЕ ЧЕРТЫ И ОСОБЕННОСТИ** 32](#_Toc103556705)

[2.1. Подход ЕС к политике кибербезопасности 32](#_Toc103556706)

[2.2. Подход НАТО к политике кибербезопасности 40](#_Toc103556707)

[**ГЛАВА 3. СОТРУДНИЧЕСТВО ЕС И НАТО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ** 49](#_Toc103556708)

[3.1. Взаимодействие НАТО и ЕС в сфере кибербезопасности на современном этапе: институционально-правовые аспекты и текущие проблемы 49](#_Toc103556709)

[3.2. Потенциал развития сотрудничества ЕС И НАТО в сфере кибербезопасности 56](#_Toc103556710)

[**ЗАКЛЮЧЕНИЕ** 64](#_Toc103556711)

[**СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ** 67](#_Toc103556712)

[**ПРИЛОЖЕНИЯ** 79](#_Toc103556713)

# **ВВЕДЕНИЕ**

Обеспечение международной безопасности сегодня является задачей всех участников международных отношений. Государства, наднациональные структуры, неправительственные организации ежедневно находятся в поиске эффективных инструментов и механизмов для реализации и защиты собственных интересов на мировой арене. Среди угроз, с которыми сталкивается международное сообщество в современном мире, выделяют дезинформацию, кибератаки, экономическое давление, в том числе санкции, вмешательство в государственные дела других стран, ассиметричное использование нерегулярных или регулярных вооруженных формирований[[1]](#footnote-2), объединяя их единым термином – гибридные.

За последние несколько лет глобальное использование информационно-коммуникационных технологий в экономике, политике, социальных отношениях стало результатом не только положительных изменений в различных сферах жизни общества, но и появления новых рисков. В связи с этим на повестку дня встает актуальный вопрос обеспечения информационной безопасности или кибербезопасности, которая, имея транснациональный характер, не может рассматриваться только на уровне отдельных государств, а требует единого ответа от наднациональных структур и иных международных институтов. Киберпространство позволяет гражданам, организациям и правительствам взаимодействовать независимо от физического местоположения. Таким образом, подобные возможности информационного пространства стирают национальные границы, создавая ситуацию, когда все участники выступают в роли равноправных сторон.

Вместе с тем, растущее число вызовов и интенсивность развития информационно-коммуникационных технологий стимулировали установление диалога между частным и государственным секторами, а также между различными международными акторами и институтами в интересах общей безопасности. Примером подобного взаимодействия является сотрудничество ЕС и НАТО по вопросам кибербезопасности. Следует признать, что на сегодняшний день обе организации играют ведущую роль в создании эффективных инструментов и выработке рекомендаций и правил для киберпространства. Основными целями обеих организаций выступают поддержание и обеспечение стабильности и безопасности в рамках трансатлантического пространства.

Уже более десяти лет организации работают над разработкой и принятием нормативных актов, в том числе и совместных, в области обеспечения информационной безопасности. В 2016 году Североатлантический Альянс принял важное решение, включив кибербезопасность в число приоритетных направлений деятельности организации. В свою очередь, государства-члены Европейского Союза, в частности, Германия, предлагают принять всеобъемлющую стратегию безопасности в рамках сотрудничества двух организаций. Однако, несмотря на то, что взаимодействие между ЕС и НАТО уже осуществляется через обмен информацией и организацию двусторонних тренингов и исследований, вопрос о формальности совместных действий остается открытым.

Таким образом, **актуальность настоящего исследования** определяется ее связью с концептуальными проблемами современных международных отношений, связанных с необходимостью выработки эффективных решений для обеспечения кибербезопасности. Изучение сотрудничества ЕС и НАТО по вопросам кибербезопасности обусловлено теоретической необходимостью оценки основных областей соизмеримости и ключевых расхождений в подходах двух акторов по отношению к политике кибербезопасности, а также выявления возможного потенциала развития этих отношений.

**Степень научной разработанности проблемы.** Международное взаимодействие по вопросам формирования архитектуры европейской безопасности в условиях возникновения угроз нового типа является одной из актуальных исследовательских проблем как в отечественной, так и в зарубежной академической и публицистической литературе. Неоднозначность политики кибербезопасности в ее понимании, различие в подходах к пониманию ее основных характеристик и субъектов определяет широкий спектр научно-теоретических и практических исследований в науке.

Прежде всего стоит обратить внимание на работы И. Уолдена, Д. Кларка, Л. Фихтнера, В. Мирона, М. Леззи, А. Коралло, Т. Стивенса, М. Карра, Кершишнига, М.М. Безкоровайного, А.Л. Татузова[[2]](#footnote-3), посвященные понятиям киберпространства, киберугроз и кибербезопасности.

В отечественной науке такие исследователи как Е.С. Зиновьева, А.А. Чеботарева, Г.А. Атаманова, Е.А. Проценко, В.Н. Лопатин, А.А. Стрельцов[[3]](#footnote-4) в своих работах рассуждают о подходах к понятию информационной безопасности, ее основных характеристиках и отличиях от исследуемого концепта кибербезопасности.

Проблеме международного сотрудничества в области обеспечения кибербезопасности посвящены работы М.Б. Касеновой, Н.В. Кардавы, А.Я. Капустина[[4]](#footnote-5), а вопросы использования информационно-коммуникационных технологий в военно-политических целях в своих работах затрагивают Л. Хенсен, М.А. Гомез, К. Вайт, Дж.Э. Митчелл, Э. Пытлак, М. Салминен, М. Керттунен, С.А. Паршин, Ю.Е. Горбачев, Ю.А. Кожанов, С.Н. Гриняев, В.Е. Макаров, С.Н. Бухарин, В.В. Цыганов[[5]](#footnote-6).

Обращаясь к предмету исследования, следует выделить работы И. Ангелова, Э. Симиона, Н. Грегер, С. Бископа, И.И. Козубенко, А.А. Буденного[[6]](#footnote-7), которые анализировали различные направления сотрудничества ЕС и НАТО в сфере безопасности и обороны.

Отдельным вопросом в зарубежных и отечественных исследованиях в рамках исследования европейской безопасности считается изучение процесса усиления роли ЕС и появления концепции стратегической автономии. Данной теме посвящены работы Дж. Хауворта, Б.Р. Поузена, Н.Ю. Тузовской, И. Щербака, Н.К. Арбатовой и А.М. Конеевой[[7]](#footnote-8).

Анализом проблем и перспектив сотрудничества ЕС и НАТО в сфере кибербезопасности занималось не так много исследователей, среди них Б. Лете, П. Перник, П. Потчев, Л.Н. Илвес, Т. Дж. Эванс, Ф. Дж. Киллуффо, А.А. Надо[[8]](#footnote-9). Чаще всего в рамках исследования информационной безопасности трансатлантического пространства затрагиваются иные вопросы, в основе которых следующие темы: сравнение подходов ЕС и НАТО к политике кибербезопасности (Л. Ковач, П. Шариков, Н. Степанова, И. Шопина, Д. Хомяков, С. Жуков, Д. Шпенов, Н. Кристинченко[[9]](#footnote-10)), кибербезопасность в политике Европейского Союза (Ф. Калдерони, Г. Кристоу, Г.Г. Фустер, Н.В. Кардава, В.И. Пантин[[10]](#footnote-11)), кибербезопасность в стратегиях НАТО (Дж. Макги, Р.Б. Хьюз, Дж. Голдгейер, А. Кемпф, А. В. Манойло, П.А, Шариков, А.В. Казаковцев, Т. Ткачук, К.П. Курылев[[11]](#footnote-12)).

В целом, наблюдается значительный пробел в исследованиях сотрудничества ЕС и НАТО в сфере кибербезопасности, в частности, в отечественной науке. Имеющаяся литература несовершенна в теоретических подходах к изучению степени угроз, которые могут быть представлены в киберпространстве, и в вопросах о том, как это новое виртуальное пространство воспринимается государствами-членами и, непосредственно, организациями – ЕС и НАТО.

**Объект** – политика кибербезопасности в рамках трансатлантического пространства.

**Предмет** – проблемы и перспективы сотрудничества ЕС и НАТО в сфере кибербезопасности.

**Цель** – на основе анализа подходов ЕС и НАТО к политике кибербезопасности определить перспективы развития их сотрудничества в данной области.

**Задачи**:

* Операционализировать понятие кибербезопасности;
* Систематизировать подходы к исследованию сотрудничества ЕС и НАТО в сфере кибербезопасности;
* Проанализировать подходы ЕС и НАТО к политике кибербезопасности;
* Исследовать общие черты и различия в подходах ЕС и НАТО к политике кибербезопасности;
* Выявить институционально-правовые аспекты и основные проблемы взаимодействия ЕС и НАТО в сфере кибербезопасности на современном этапе;
* Определить возможные перспективы развития сотрудничества ЕС и НАТО в сфере кибербезопасности.

**Основная научная гипотеза исследования** состоит в том, что между ЕС и НАТО возможно дальнейшее расширение и углубление сотрудничества с учетом наличия общих ценностей и способов реализации защиты критической инфраструктуры и обеспечения стабильности в киберпространстве в рамках подходов организаций к политике в данной области. При этом каждый из акторов преследует собственные цели и задачи в рамках обеспечения кибербезопасности, получая индивидуальные выгоды от сотрудничества.

**Вторая научная гипотеза** состоит в том, что дальнейшее построение общей политики кибербезопасности не представляется возможным по причине принципиальных различий в подходах ЕС и НАТО, а также из-за продолжающегося дублирования функций. ЕС продолжит предпринимать соответствующие шаги для установления собственной независимости в сфере безопасности и утверждения стратегической автономии от НАТО.

**Хронологические рамки** охватывают период с 2007 г., когда после кибератаки в Эстонии кибербезопасность стала стратегическим вопросом в трансатлантическом регионе, по настоящее время с возможностью определения перспектив развития сотрудничества ЕС и НАТО. Для решения поставленных задач исследования был взят более широкий исторический контекст – с 1999 по настоящее время.

**Территориальные рамки** не ограничиваются странами-членами ЕС (27 государств) и НАТО (30 государств), а включают также регионы мира, которые непосредственно связаны с деятельностью организаций в сфере кибербезопасности.

**Теоретико-методологическая база исследования** основана на междисциплинарном подходе, который позволил провести комплексный анализ сотрудничества ЕС и НАТО в сфере кибербезопасности.

***Теория секьюритизации*** Копенгагенской научной школы **(**Б. Бузан, О. Вевер, Я. Уайлд[[12]](#footnote-13)**)** позволила концептуализировать термины киберпространства, киберугрозы и кибербезопасности, определить референтные объекты информационной безопасности и кибербезопасности, угрозы и направления оптимизации деятельности по защите киберпространства, а также применить данные понятия к политике кибербезопасности в рамках ЕС и НАТО.

***Пространственный подход***[[13]](#footnote-14) помог выявить субъекты трансатлантического пространства безопасности как одной из форм транснационального политического пространства, провести анализ причин формирования сотрудничества ЕС и НАТО в сфере кибербезопасности, изучить развитие отношений двух структур, институционализацию их связей, а также формирование новых пространств в рамках создания специализированных учреждений и закономерности поведения акторов внутри пространства, основываясь на их подходах к киберполитике.

***Системный подход*** (в интерпретации А.А. Богданова[[14]](#footnote-15)) позволил изучить трансатлантическую систему кибербезопасности с точки зрения ее структуры, внутренней иерархии, места в системе международных отношений.

Наконец, основываясь на теории ***неоинституционализма рационального выбора***[[15]](#footnote-16), был проведен сравнительный анализ интересов, целей и задач, инструментов, ресурсов ЕС и НАТО с целью определения проблем, способных помешать процессу сближения в области кибербезопасности, и оценки взаимодополняемости обеих организаций для дальнейшего расширения сотрудничества в области информационной безопасности.

Для реализации поставленных задач в рамках исследования были использованы следующие методы: ***исторический подход***, с помощью которого была проанализирована эволюция развития сотрудничества ЕС и НАТО в сфере кибербезопасности в заданный промежуток времени (1999 – наст. время); ***структурно-институциональный анализ***, который позволил изучить внутреннее устройство систем обеспечения кибербезопасности в ЕС и НАТО; ***сравнение*** подходов ЕС и НАТО к политике кибербезопасности; ***качественный контент-анализ***, благодаря которому были выявлены цели, задачи и определены основные практики и направления реализации политики информационной безопасности ЕС и НАТО на основе анализа официальных документов, аналитических материалов и сайтов организаций; ***метод построения прогнозных сценариев***, позволивший определить перспективы развития сотрудничества ЕС и НАТО в сфере кибербезопасности.

**Научная новизна исследования** заключается в комплексном анализе сотрудничества ЕС и НАТО в сфере кибербезопасности, как отдельном направлении совместной деятельности двух акторов в рамках общей политики безопасности. На основе сравнительного анализа были выявлены особенности подходов организаций к политике кибербезопасности по нескольким аспектам. Метод построения прогнозных сценариев, реализованный благодаря проведению качественного контент-анализа и анализа факторов прошлого и современного состояния сотрудничества структур, позволил определить три возможных вектора дальнейшего развития отношений ЕС и НАТО в сфере киберзащиты: 1) расширение и углубление взаимодействия; 2) статус-кво в отношениях; 3) деградация и неэффективность совместной деятельности.

**Источниковая база исследования** может быть разделена на три основные группы, каждая из которых имела свое значение в рамках исследовательской работы.

*Первую группу* составляют стратегические документы Европейского Союза и НАТО[[16]](#footnote-17), анализ которых позволил решить ряд задач. Во-первых, выявить общие и различающиеся угрозы кибербезопасности для ЕС и НАТО, а также отличительные черты в подходах к их определению и степени значимости. Во-вторых, в стратегиях напрямую отражены интересы и цели ЕС и НАТО, что позволило как определить их субъектность на международной арене, так и на основе анализа приоритетов обеих организаций в сфере кибербезопасности прогнозировать их будущие отношения.

Ко *второй группе* относятся официальные документы, доклады и материалы ЕС и НАТО в области безопасности. Во-первых, это учредительные документы, среди которых Североатлантический договор[[17]](#footnote-18), Договор о Европейском союзе[[18]](#footnote-19), Договор о функционировании Европейского союза[[19]](#footnote-20) и Лиссабонский договор[[20]](#footnote-21). Во-вторых, это документы и официальные публикации[[21]](#footnote-22), декларации саммитов НАТО на различных уровнях[[22]](#footnote-23). В-третьих, это двусторонние договоры, соглашения и совместные декларации ЕС и НАТО[[23]](#footnote-24), на основе которых строится сотрудничество структур. Анализ этой группы документов позволил изучить подходы ЕС и НАТО, различия между ними, а также проследить развитие политических дискурсов, появление новых региональных повесток. Кроме того, в этих документах раскрывается политическая и организационная сущность институтов и механизмов, связанных с кибербезопасностью.

*Третью группу* составляют материалы с официальных сайтов ЕС и НАТО, их учреждений и агентств и пресс-релизы о событиях, имеющих отношение к политике кибербезопасности организаций как по отдельности, так и в рамках сотрудничества[[24]](#footnote-25). Источники из этой группы позволили комплексно рассмотреть проблему исследования и решить поставленные задачи. В дополнение к трем группам к данному разделу следует отнести результаты эмпирического исследования, проведенного при непосредственном участии автора (контент-анализ, 2021–2022 гг.[[25]](#footnote-26)).

**Теоретическая и практическая значимость исследования** заключается в возможности его использования в политико-аналитической деятельности. Проведенный анализ стратегических документов международных организаций в области информационной безопасности может быть учтен при разработке российских доктрин, стратегий и законодательных актов, а также в рамках повышения уровня защиты критической инфраструктуры в киберпространстве межправительственных структур, в которые входит Российская Федерация (ЕАЭС, ОДКБ, СНГ, ШОС, СГ и другие). Проведенный комплексный анализ политики обеспечения кибербезопасности демонстрирует расстановку политических сил в глобальном информационном пространстве. Выводы исследования могут быть полезны аналитическим ведомствам для оценки и прогноза внешнеполитической деятельности государств в виртуальном поле.

Материалы данного исследования могут быть использованы в процессе организации самостоятельной работы студентов направлений 41.03.05 Международные отношения (бакалавриат) и 41.04.05 Международные отношения (магистратура), а также при подготовке к семинарским занятиям по курсам «Актуальные проблемы Общей внешней политики и политики безопасности ЕС», «Международные организации», «Региональные организации Европы», «Информационное общество и международные отношения», «Интернет и мировая политика в XXI веке».

**Структура работы** определяется поставленными задачами. Работа состоит из введения, трех глав, включающих в себя подразделы, заключения, списка использованной литературы и источников и приложений. Каждая глава посвящена определенному фрагменту изучаемой темы и имеет завершающие логические выводы.

Во **введении** обосновывается актуальность выбранной темы исследования, описываются цели и задачи работы, а также объект и предмет, указываются хронологические и территориальные рамки, теоретические и методологические основы, предоставляется характеристика примененной источниковой базы и библиографический анализ темы исследования.

**Первая глава** состоит из двух подразделов, в первом из которых анализируются подходы к понятию кибербезопасность, во втором – на основе изучения работ зарубежных и отечественных исследователей определяются основные тенденции в исследованиях сотрудничества ЕС и НАТО в сфере кибербезопасности.

**Вторая глава** также включает два подраздела, в каждом из которых проводится комплексный анализ подходов ЕС и НАТО к политике кибербезопасности, а в результате производится их сравнительный анализ.

**Третья глава** посвящена современному состоянию и перспективам развития сотрудничества ЕС и НАТО в киберсфере. Первый подраздел описывает основные достижения организаций в области реализации совместной политики кибербезопасности и существующие проблемы, второй – сценарии развития отношений в данной сфере.

В **заключении** представляются конкретные выводы, полученные в результате исследования данной темы.

**Апробация работы.** Основные положения и результаты исследования были апробированы автором в рамках участия в Международной научной конференции молодых ученых «Европа после 2020» (Томск, 2021), II научной конференции студентов и молодых ученых «Orbes Politici» Школы политических исследований ИОН РАНХиГС (Москва, 2021), «Зимней конференции СНО: тренды и вызовы современной дипломатии» (Санкт-Петербург, 2021). Выводы данной работы нашли свое отражение в научных публикациях автора[[26]](#footnote-27).

# **ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ СОТРУДНИЧЕСТВА НАТО И ЕС В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ**

## **1.1. Политика кибербезопасности как объект научного анализа**

Стремительное развитие и распространение информационно-коммуникационных технологий (ИКТ) изменило различные сферы жизни. Процесс глобальной информатизации на сегодняшний день является одной из доминирующих тенденций XXI века. Вместе с тем, преимущества технологий, которые используются как в повседневной жизни, так и на государственном и международном уровне, сопровождаются угрозами, исходящими из различных источников.

За последнее время следует отметить значительный среднегодовой рост числа инцидентов в области ИКТ, которые затрагивают не только частные интересы, но и государственную инфраструктуру. В частности, в 2021 году организацией IT Governance было зафиксировано более 5 млрд. нарушений в киберпространстве, связанных с созданием вредоносного программного обеспечения, несанкционированным доступом и кражей личных данных, фишинговыми атаками и другими незаконными действиями[[27]](#footnote-28). По мнению С.Н. Гриняева, информационное пространство условно можно разделить на информационно-психологическую и техническую составляющие, на традиционные средства передачи информации (газеты, радио, телевидение) и киберпространство. Последнее становится центральным сегментом в современном процессе передачи информации, так как постепенно поглощает другие его элементы[[28]](#footnote-29).

Между тем сегодня ни у кого не вызывает сомнений, что использование информационно-коммуникационных технологий имеет международное значение в связи с его трансграничным характером. Международное сообщество признает важную роль Интернета, поэтому все чаще мы можем наблюдать заключение межнациональных соглашений и создание межправительственных связей, главная цель которых состоит в определении границ нового виртуального пространства и зон ответственности, а также формировании единого подхода к обеспечению безопасности и построении глобального информационного общества[[29]](#footnote-30).

Следовательно, действия по защите критической инфраструктуры, а именно обеспечение кибербезопасности, становятся крайне популярны в государственной и корпоративной деятельности. Более того, существуют иные причины возросшего внимания к созданию условий для безопасного функционирования информационно-коммуникационных технологий.

Во-первых, на государственном и наднациональном уровнях сбор и обработка информации становятся первостепенными задачами, поскольку акторы международных отношений испытывают потребность в обладании достоверными данными о существующем положении дел в мире. Для этого создаются специализированные системы, которые благодаря компьютерным технологиям непрерывно наблюдают за окружающей обстановкой, при этом требуя высоких стандартов безопасности.

Во-вторых, свойства и инструменты информационного пространства широко используются в военно-политической сфере. В новом информационном обществе изменяется тип ведения войн: они становятся автоматизированными в рамках управления вооруженными силами государства, которые располагаются в различных точках региона или мира. Вводится новое понятие – информационная война, – заключающееся в управлении восприятием событий со стороны средств массовой информации.

Наконец, технологии киберпространства применяются в стратегических отраслях экономики, а также для обеспечения работы государственных и иных структур. Следуя из этих данных, можно сделать вывод о том, что киберпространство оказывается связанным со всеми сферами жизни общества, и для эффективного функционирования технологий необходимо ответственно подходить к выбору инструментов их защиты.

Прежде чем продолжить рассмотрение конкретных примеров обеспечения кибербезопасности, обратимся к теоретической составляющей термина. Следует сразу отметить, что понятие «кибербезопасность» с одной стороны представляется субъективным, однако, с другой стороны, определив рамки исследования данного концепта, можно выявить его объективные стороны. Деконструкция термина позволяет рассмотреть его с точки зрения двух дефиниций: «cyber» и «security». «Кибер» – это приставка, обозначающая информационное пространство (cyberspace), относящееся к сетям электронной связи и виртуальной реальности[[30]](#footnote-31). Оно происходит от термина «кибернетика», который относится к процессам управления сложными динамическими системами, а также получения, хранения, преобразования и передачи информации в рамках этих систем. Впервые понятие «cyberspace» было употреблено писателем-фантастом Уильямом Гибсоном в романе «Нейромант», в котором он описывает свое видение трехмерного пространства компьютерных систем, содержащих информацию, а людей в роли генераторов и пользователей этих данных[[31]](#footnote-32).

Соответственно, можно сделать вывод, что киберпространство не статично и не однородно, а обладает несколькими уровнями. Согласно американскому ученому в области информатики Дэвиду Кларку и примененному им системному подходу, существует четыре уровня киберпространства: физический, то есть вся материальная инфраструктура, являющаяся «фундаментом» киберпространства; логический, включающий алгоритмы, то есть внутреннюю «природу» информационного пространства; информационный – непосредственно информация, которая хранится, передается и преобразуется в этой системе; и социальный, относящийся к пользователям и создателям информационных кластеров[[32]](#footnote-33).

Определение «security» или «безопасности» достаточно сложно привести к общему знаменателю. Теоретики копенгагенской школы Б. Бузан, О. Вевер, Я. Уайлд полагают, что безопасность может быть определена различными способами. Они утверждают, что само понимание безопасности устойчиво, а характер угроз и ключевые объекты могут изменяться. Так, в качестве референтного объекта, то есть актора, на которого может быть направлена угроза безопасности, который уже имеет политический характер и находится на этапе секьюритизации, может выступать глобальное информационное пространство[[33]](#footnote-34). В данном контексте представляется возможным рассмотреть понятие «кибербезопасность» в точки зрения четырех подходов:

***1. Кибербезопасность как защита персональных данных.***

В данном случае в качестве угроз могут выступать неправомерные действия хакеров, стремящихся получить конфиденциальную информацию с целью взлома системы, а также деятельность правительств или корпораций, собирающих личные данные о гражданах. Объединяющим элементом в подходах к кибербезопасности как защите данных является цель такой деятельности, заключающаяся в создании эффективных мер для предотвращения угроз незаконного или необоснованного доступа к конфиденциальной информации. Подобными мерами может стать принятие законов о защите личных данных. Например, в рамках ЕС действует Общий регламент, который устанавливает правила, которым следуют корпорации при обработке данных о гражданах. Более того, в тех случаях, когда речь идет о преступной деятельности, к расследованию незаконных актов могут быть привлечены правоохранительные органы[[34]](#footnote-35).

***2. Кибербезопасность как защита экономических интересов.***

В этом случае считается, что кибербезопасность управляется рынком, то есть она обеспечивает соблюдение существующих экономических правил и законов, а также защищает честную конкуренцию и принципы рыночной экономики. Потенциальные угрозы могут исходить от киберпреступников, компаний-конкурентов, правительств других государств, политических групп и активистов. Большинство компаний используют ИКТ для организации бизнес-процессов и хранения информации в цифровом виде. Защита этих систем от потенциальных злоумышленников гарантирует экономические преимущества. Кроме этого, кибербезопасность может быть связана с защитой критической инфраструктуры, как, например, общественный транспорт или здравоохранение. В таком случае кибератаки могут не только нанести ущерб потребителям, но и привести к потере доверия к компании. Примером кибербезопасности как защиты экономических интересов является обеспечение соблюдения цифровых авторских прав. В частности, «Закон об авторском праве в цифровую эпоху»[[35]](#footnote-36), принятый в 1998 г. в США, обеспечивает защиту обладателям авторского права, чей материал опубликован в сети Интернет[[36]](#footnote-37).

***3. Кибербезопасность как защита общественно-политической инфраструктуры.***

С распространением информационно-коммуникационных технологий все больше общественных и жизненно важных структур подключаются к сети Интернет. Угрозы в таком случае носят политически мотивированный характер и исходят от политизированных или военных групп, активистов или целых государств. Следовательно, объектами секьюритизации часто выступают военные подразделения и международные военные альянсы, а также национальные правоохранительные органы и спецслужбы. Примером подобных угроз является вирус Stuxnet, который использовался для выведения из строя промышленных объектов в Иране, в том числе завода по обогащению урана[[37]](#footnote-38). В рамках этого подхода возможные ответные меры могут включать разработку систем безопасности, мониторинг сети и передачи данных. В некоторых случаях могут применяться наступательные стратегии или дипломатические инструменты[[38]](#footnote-39).

***4. Кибербезопасность как контроль над информацией и коммуникациями.***

Данный подход фокусируется на использовании информационно-коммуникационных систем для различных целей, включая политическую активность, противостояние политическим режимам, распространение агитационных посланий и пропаганды, а также организации преступной деятельности. В этом случае в центре внимания оказываются два аспекта по контролю за коммуникационными потоками: во-первых, это наблюдение за интернет-дискуссиями и сбор разведданных с целью выявления потенциальных угроз, и, во-вторых, использование методов слежения с целью прямой модерации и цензуры той информации, которую распространяют в сети Интернет. Чаще всего подобные меры мотивированы такими ценностями как национальная безопасность, верховенство закона, общественная безопасность и политическая стабильность.

Таким образом, кибербезопасность может быть представлена с точки зрения различных подходов, однако в любом случае все они взаимосвязаны и образуют единую систему обеспечения безопасности в информационном пространстве с целью защиты личных, государственных и частных интересов.

Важным аспектом в исследовании дефиниции «кибербезопасность» является ее сравнение с не менее известным понятием «информационной безопасности». В отечественных исследованиях полагают, что термин «кибербезопасность» может быть использован исключительно для описания технологических аспектов в процессе обеспечения защиты киберпространства, в то время как «информационная безопасность» включает еще и широкий спектр вопросов, связанных с обеспечением информационно-психологической стабильности и регулированием информационных потоков в сети Интернет[[39]](#footnote-40). Возвращаясь к теории секьюритизации, следует сказать и о различиях терминов с точки зрения определения их референтных объектов: в первом случае таковыми являются безопасность информационных сетей и систем (другими словами, защита критической инфраструктуры), во втором случае – обеспечение информационного суверенитета. Общей характеристикой для обоих терминов выступает наличие у них связи с переходом к информационной эпохе развития общества, когда главные угрозы безопасности стали рассматриваться как порожденные и усиленные в результате всеобщей информатизации.

В зарубежных исследованиях и на практике также прослеживается два подхода к определению данного термина. В рамках широкого подхода понятие кибербезопасности включает в себя как технические, так и психологические аспекты. Узкий подход ограничивается исключительно аспектами технического характера. К примеру, в стратегии Швеции под кибербезопасностью понимается комплекс мер безопасности, направленных на сохранение конфиденциальности, достоверности и доступности информации[[40]](#footnote-41). В свою очередь Германия в стратегии кибербезопасности использует узкий подход, где кибербезопасность определена как желаемая цель информационной безопасности, ситуация, в которой риски немецкого киберпространства были уменьшены до приемлемого минимума[[41]](#footnote-42).

Несмотря на наличие двух направлений изучения и использования термина, в литературе можно встретить исследования, где понятие «информационной безопасности» полностью соответствует определению «кибербезопасности». Британский исследователь Т. Стивенс пишет о кибербезопасности не только как о средстве защиты общества и его информационной инфраструктуры, но и как о способе преследования государственных и международных политических деятелей с помощью информационно-технологических средств. Это, по мнению теоретика, подчеркивает онтологический характер кибербезопасности и способность инструментов киберпространства добиваться политического эффекта посредством транснационального вмешательства через Интернет[[42]](#footnote-43). М.А. Гомез и К. Уайт придерживаются схожей позиции, заявляя о том, что влияние новых обстоятельств окружающей среды на формирование общественного мнения определяется включенностью людей в современное цифровое общество, поэтому уникальные характеристики киберпространства имеют определяющее значение в процессе формулирования общего ответа от общества, а значит кибербезопасность имеет в том числе и информационно-психологический характер[[43]](#footnote-44).

Доктор юридических наук Чеботарева А.А. придерживается философского подхода, который основывается на выделении трех взаимосвязанных элементов при концептуализации термина: удовлетворение информационных потребностей субъектов; безопасность информации; защита субъектов[[44]](#footnote-45). В таком случае, информационная безопасность связана с состоянием объекта, когда условия информационной среды позволяют принимать и реализовывать решения сообразно целям объекта[[45]](#footnote-46). Подход, основанный на технологических аспектах, затрагивает проблему разработки стандартов, обеспечивающих защиту серверов, сертификацию объектов информатизации, использование систем криптографии для передачи данных[[46]](#footnote-47).

О триаде составляющих элементов кибербезопасности рассуждают М.М. Бескоровайный и А.Л. Татузов, выделяя следующие составные части киберпространства: информационные ресурсы, компьютерная и сетевая инфраструктура и способы взаимодействия пользователей. Согласно данному подходу, кибербезопасность включает и информацию в качестве объекта защиты, и средства, определяющие факторы ее функционирования, и защиту способов жизнеобеспечения виртуального пространства[[47]](#footnote-48).

Лопатин В.Н. пишет об информационной безопасности как о состоянии защищенности определяющих интересов личности, общества и государства от негативного воздействия[[48]](#footnote-49). Этот термин перекликается с традиционным понятием безопасности и может включать любые аспекты кибербезопасности: начиная от технологических и заканчивая психологическими. Доктор технических наук, бывший заместитель начальника Управления информационной безопасности аппарата СБ РФ А.А. Стрельцов говорит об информационной безопасности как о сложном процессе, включающем информационные потребности государства, деятельность по удовлетворению этих потребностей, угрозы безопасности и процесс противодействия им[[49]](#footnote-50).

Что же касается употребления термина «информационная безопасность» в стратегических и законодательных документах Российской Федерации, то для обозначения защиты информационного пространства используется различная терминология[[50]](#footnote-51). Чаще всего можно встретить термин «информационная безопасность», так как это более широкое определение всевозможных угроз для критической инфраструктуры и информационного поля. Такие различия во многом обусловлены релевантностью их перевода на национальный язык. Вместе с тем, в зарубежной литературе, в том числе и в нормативно-правовых актах других государств, в большей степени встречаются термины, содержащие приставку «кибер».

Таким образом, поскольку в научной среде нет единого определения термина «кибербезопасность», то в настоящей работе будет использована следующая авторская формулировка, объединяющая различные подходы, описанные выше: кибербезопасность – это совокупность технологий, процессов, практик и мер реагирования, предназначенных для защиты информационно-коммуникационных систем, в том числе компьютеров, программ и данных, от повреждения, несанкционированного использования и модификации с целью обеспечения их конфиденциальности и целостности. В данном исследовании автор только частично затронет вопросы информационно-психологической составляющей кибербезопасности с целью избежать субъективности, поскольку вопросы информационной пропаганды и распространения дезинформации чаще всего не имеют объективного основания.

## **1.2. Подходы к изучению взаимодействия НАТО и ЕС по вопросам кибербезопасности**

Деятельность, осуществляемую в киберпространстве, достаточно сложно регулировать, поскольку информационное поле не имеет границ и распространено повсеместно. В зарубежных и отечественных исследованиях идут дискуссии о том, где заканчивается ответственность одних действующих в киберпространстве акторов и начинается зона ответственности других, так как проблемы и угрозы, которые возникают в этой плоскости, слишком масштабны и их сложно контролировать только лишь на государственном уровне. В связи с этим возникает необходимость межгосударственного сотрудничества, а также выстраивания общих направлений деятельности в сфере обеспечения кибербезопасности между различными международными институтами.

Европейский Союз и НАТО занимают лидирующие позиции в мире по разработке эффективных мер противодействия киберугрозам. В научном дискурсе часто анализируются стратегии национальной безопасности государств-членов и их влияние на работу межправительственных организаций, однако тема сотрудничества ЕС и НАТО в конкретных направлениях остается не полностью раскрытой.

Обе структуры разделяют идеи поддержания стабильности, обеспечения мира и безопасности для своих граждан. Это во многом объясняется тем, что большинство членов ЕС и НАТО одинаковы: 21 из 30 союзников по НАТО имеют членство в ЕС. Традиционно считается, что НАТО как военно-политический блок обеспечивает сотрудничество в области военной стабильности и безопасности, а ЕС несет ответственность за эффективное функционирование экономики стран-членов и обеспечение основных свобод, необходимых для устойчивого развития. При этом, обе организации не взаимоисключают друг друга: вступая в ЕС, государства отдают часть своего суверенитета в обмен на общий рынок, свободу передвижения людей, товаров и услуг, а также финансовую и структурную поддержку; союзники по НАТО, согласно 5 статье Североатлантического договора, получают гарантии защиты со стороны всех стран-членов в случае нападения.

Долгое время государства-члены обеих организаций выражали общее мнение о том, чтобы оставаться разделенными на основе своих идей и стратегических целей. Однако, сложность проблем, включающих возникновение гибридных угроз, в том числе в киберпространстве, поставила вопрос о необходимости сотрудничества между ЕС и НАТО, между частными и государственными секторами, гражданским обществом, бизнес-структурами и правительствами стран-членов[[51]](#footnote-52). Анализ деятельности ЕС и НАТО в сфере безопасности позволяет сделать вывод о том, что обе структуры придают первостепенное значение устойчивости и защите своих информационных сетей.

Несмотря на то, что кибербезопасность отдельных государств-членов остается национальной ответственностью, действия организаций в сфере обеспечения информационной безопасности гармонично дополняют друг друга: НАТО акцентирует внимание на аспектах, связанных с технологическими элементами безопасности и обороны, а ЕС занимается более широким кругом невоенных вопросов (свобода и управление Интернетом, защита данных и прав граждан в виртуальном пространстве), а также внутренней безопасностью[[52]](#footnote-53). Исследователь И. Уолден отмечает, что в кибербезопасности не существует разделения на военные и гражданские цели[[53]](#footnote-54), именно поэтому киберпространство может стать либо возможностью для расширения взаимодействия, либо причиной для конфликта. В настоящем исследовании речь пойдет о первом случае, а именно об углублении сотрудничества ЕС и НАТО в сфере кибербезопасности.

Академическая литература о взаимодействии ЕС и НАТО в области безопасности в основном сосредоточена вокруг двух направлений: сотрудничество ЕС и НАТО в сфере обороны и безопасности и дискуссии о стратегической автономии ЕС. Дж. Хауворт вводит понятие «дилемма евроатлантической безопасности», которое иллюстрирует внутреннюю напряженность в ЕС по вопросу о необходимости наращивания военного и оборонного потенциала[[54]](#footnote-55). Великобритания, будучи членом ЕС, настаивала на том, что стремление Европы к автономии может вызвать негативную реакцию со стороны Соединенных Штатов. Напротив, Франция утверждала, что США будут приветствовать решение стран-членов ЕС[[55]](#footnote-56). Возникшая напряженность также подкреплялась двусмысленной позицией американского правительства, которое, с одной стороны, поощряло действия и решения ЕС о развитии оборонного потенциала в целях защиты региона, а с другой стороны, выражало опасения на счет того, что однажды Европа получит возможность бросить вызов американским коллегам в военном плане[[56]](#footnote-57). В целом, Дж. Хауворт в своих рассуждениях приходит к выводу о будущей несостоятельности Североатлантического альянса и цитирует слова Д. Эйзенхауэра о том, что «[если] НАТО все еще будет нужен через 10 лет, то потерпит неудачу в своей деятельности»[[57]](#footnote-58).

В отечественных исследованиях также затрагивается тема стратегической автономии ЕС. Тузовская Н.Ю. обращает внимание на противоречивый характер отношений ЕС и НАТО. С одной стороны, между структурами наблюдается сближение позиций, в то же время с другой стороны – из-за несовпадения взглядов, еще большего стремления ЕС к автономии, а также институционально заложенного дублирования ряда функций постепенно усиливается конкуренция. Однако, динамика развития этих отношений дает возможность полагать, что от прежней зависимости ЕС от НАТО отношения переходят к стадии взаимозависимости[[58]](#footnote-59). И. Щербак в своей статье анализирует влияние пандемии на возможность мобилизации ресурсов ЕС в рамах усиления его глобальной роли, что в результате позволило сформировать концепцию стратегической автономии. В исследовании говорится о том, что Брюссель интегрировал данную концепцию практически во все направления своей внешнеполитической и внутриполитической деятельности: начиная от создания условий для эффективного обеспечения защиты населения («суверенное здравоохранение») и заканчивая автономией в развитии технологий и искусственного интеллекта. При этом противоречия в отношениях между США и КНР, по мнению И. Щербака, Евросоюз использует для выбора потенциального партнера, а значит цель сотрудничества с НАТО может отойти на второй план[[59]](#footnote-60). Наконец, о стратегической автономии ЕС в своей монографии пишут Н.К. Арбатова и А.М. Кокеева, рассуждая о внешнеполитическом контексте развития ЕС, ставшего катализатором ряда инициатив стран-членов, включая Глобальную стратегию безопасности, создание Постоянного структурированного сотрудничества (PESCO), формирование структуры военного планирования и обеспечения боеспособности за пределами зоны ответственности ЕС (MPCC) и других[[60]](#footnote-61).

И. Ангелов, напротив, рассуждает об экономических перспективах сотрудничества ЕС и НАТО в области обороны и безопасности. Исследователь утверждает, что из-за меняющейся международной обстановки, появления гибридных угроз в таких сферах как киберпространство или энергетика, возникает разрыв между «старыми» и «новыми» странами-членами ЕС с точки зрения их оборонных возможностей и ресурсов. Именно поэтому обеспечение скоординированного подхода ЕС-НАТО к политике безопасности является первостепенной задачей для государств[[61]](#footnote-62). Э. Симион также утверждает, что ЕС и НАТО достигли такого уровня взаимопонимания, что могут совместно справиться с новыми угрозами в сфере безопасности[[62]](#footnote-63). Кроме того, Н. Грегер, рассматривая взаимодействие двух акторов через призму микроанализа, обнаруживает, что в отношениях ЕС и НАТО происходит постепенный переход от формального к неформальному сотрудничеству: например, между военным и гражданским персоналом, дипломатами и другими представителями обеих структуру[[63]](#footnote-64).

Говоря о существующих проблемах и способах их решения, следует выделить статью С. Бископа, который приходит к выводу о том, что для эффективного взаимодействия, с одной стороны, НАТО должен признать приоритет использования существующих инструментов Евросоюза в целях достижения общих оборонных целей, а, с другой стороны, ЕС должен начать рассматривать PESCO не как способ проведения малоинтенсивных операций, которые имелись в арсенале организации и до этого, а как механизм устранения недостатков в европейских вооруженных силах в целом и сближения с потенциалом НАТО[[64]](#footnote-65).

Из российских исследователей И.И. Козубенко рассуждала о потенциальных возможностях расширения сотрудничества ЕС и НАТО в сфере безопасности. Основываясь на положениях соглашения «Берлин Плюс», профессор делает вывод о том, что организации выработали эффективную стратегию взаимодействия, которая облегчает делегирование полномочий, оптимизирует ресурсы обеих структур и помогает избежать дублирования функций[[65]](#footnote-66). Более того, в отечественной науке в сравнении с исследованиями, посвященными сотрудничеству ЕС-НАТО, существенно шире освещены вопросы взаимоотношений США и Канады со странами-членами ЕС или организацией в целом. В частности, А.А. Будённый приходит к выводу о том, что о полной европейской автономии в сфере безопасности говорить рано, так как Европа еще остается ближайшим партнером США, а ЕС и НАТО на современном этапе развития следует рассматривать скорее с позиции «комплексной взаимозависимости», а также как акторов, нуждающихся в поиске внутреннего консенсуса в рамках трансатлантического пространства[[66]](#footnote-67).

Следовательно, возможности расширения сотрудничества между ЕС и НАТО должны быть транслированы на все угрозы, с которыми сталкиваются акторы, в том числе, и на киберсферу. Зарубежные и отечественные исследования по вопросам взаимодействия ЕС и НАТО в сфере обеспечения кибербезопасности также ограничены и в основном содержат лишь анализ существующих проблем. Л. Ковач приводит сравнение стратегии кибербезопасности ЕС с политикой киберзащиты НАТО[[67]](#footnote-68), однако в исследовании отсутствует теоретическое обоснование взаимодействия акторов. Б. Лете и П. Перник дают краткий обзор сотрудничества ЕС и НАТО в сфере киберпространства, а также проблем, с которыми они сталкиваются в этой области, и направлений их решения, содержащих рекомендации о повышении осведомленности и обмене информацией[[68]](#footnote-69).

Другая часть исследований включает аргументы в пользу сотрудничества ЕС и НАТО в киберпространстве и важность скоординированного подхода в этой области. Так, П. Перник подчеркивает необходимость более тесного взаимодействия двух организаций и проводит анализ того, как киберугрозы впервые были представлены каждым из акторов и как они эволюционировали в рамках разработки всеобъемлющей политики кибербезопасности[[69]](#footnote-70). Необходимость расширения взаимодействия подчеркивает П. Поптчев, заявляя, что сотрудничество ЕС и НАТО в сфере кибербезопасности может быть полезно по причине схожих политических интересов и технологических возможностей. Так, в Стратегии кибербезопасности США утверждается, что европейские союзники и партнеры обладают большим потенциалом в области кибернетики, поэтому общие угрозы структур должны стать поводом для углубления партнерских отношений посредством трансграничных обменов, доступа к информационным базам в сфере промышленности и взаимодействия с научным сообществом и компаниями в области информационно-коммуникационных технологий[[70]](#footnote-71).

В отечественной науке приоритетным направлением для анализа становится сравнение подходов США, ЕС, НАТО и России к политике информационной безопасности. Так, П. Шариков и Н. Степанова приходят к выводу о том, что складывание информационной политики в рамках европейского вектора происходило под влиянием американской традиции, поэтому несложно догадаться, что наиболее эффективные элементы опыта США в области регулирования сферы ИКТ перешли в стратегии кибербезопасности ЕС[[71]](#footnote-72). Таким образом, синергия европейского и американского подходов к политике кибербезопасности позволяет говорить о схожих целях и задачах акторов в данной сфере. Н.В. Кардава в своей статье о национальном и наднациональном уровнях информационной политики ЕС рассуждает о проблемах организации в рамках обеспечения безопасности информационного пространства, связанных с дублированием функций в области кибербезопасности с НАТО[[72]](#footnote-73).

В целом, прослеживается значительный пробел в теоретических подходах к изучению степени угроз, которую представляет область кибербезопасности, и в том, как это новое виртуальное пространство воспринимается государствами членами и, непосредственно, организациями – ЕС и НАТО. Имеющаяся литература несовершенна в рамках концептуализации исследуемого пространства из-за его особенностей в стирании границ между военным и гражданским направлениями. В связи с этим следует определить теоретические рамки настоящей работы.

Исследователи, изучающие характер внешней политики и политики европейской безопасности, представляют различные теоретические школы. Они опираются как на общие теории международных отношений, так и на теории европейской интеграции. Большой вклад в изучении общей внешней политики и политики безопасности ЕС, помимо традиционных дискуссий вокруг реализма и либерализма, вносят конструктивисты и институционалисты. Однако, поскольку в исследовании речь идет не только о внешней политике ЕС, но и его взаимодействии с военно-политическим блоком НАТО, для изучения данной темы будет использован междисциплинарный подход, включающий несколько теоретических направлений.

В первую очередь, следует согласиться с теми исследователями, которые обращаются к пространственному подходу в рамках изучения межрегионального сотрудничества. И.Л. Прохоренко под политическим пространством понимает организационную конфигурацию политической жизни, форму, которая выражает определенные устойчивые отношения между индивидуальными и коллективными субъектами политического процесса[[73]](#footnote-74). В рамках международных отношений можно также наблюдать формирование политических пространств, в основе которых лежит транснациональное сотрудничество, осуществляемое от лица национальных или наднациональных структур. Н.А. Косолапов рассматривает международный регион как одну из форм транснационального политического пространства, а также комплекс регулярных и устойчивых связей[[74]](#footnote-75). Следовательно, появление транснациональных связей, с одной стороны, приводит к появлению устойчивых институциональных образований, а с другой – к формулированию общих норм и правил, созданию совместных целей и задач, определению универсальных ценностей для конкретного политического пространства.

В соответствии с данным подходом представляется возможным рассматривать зону сотрудничества ЕС и НАТО, а именно трансатлантический регион, в категориях транснационального политического пространства. Пространственный подход позволит исследовать развитие отношений двух структур, институционализацию их связей, формирование новых пространств в рамках создания специализированных учреждений сотрудничества в области кибербезопасности, а также закономерности поведения акторов внутри пространства, основываясь на их подходах к киберполитике.

В дополнение к имеющемуся важным представляется использование системного подхода в интерпретации А.А. Богданова, который предложил концепцию всеобщей организационной науки – тектологии. В политической науке системный подход применялся в исследованиях выдающихся теоретиков, среди которых Т. Парсонс, Н. Луман, К. Дойч, Г. Алмонд, Д. Истон, М. Каплан. Каждый из них по-разному определял концепт системы. Например, американский профессор политических наук М. Каплан ассоциировал международные отношения с открытой системой, свойства частей которой не сводятся к свойствам целого[[75]](#footnote-76). Д. Истон, американский политолог, указывал на динамичность структуры международных отношений и, следовательно, на постоянное изменение акторов, которые оказывают влияние на систему мировой политики[[76]](#footnote-77). Концептуализацией системного подхода в рамках отечественной научной школы занимался А.Д. Богатуров, который предлагал понимание системы международных отношений в качестве принципа или закона взаимосвязи различных государств и наднациональных структур[[77]](#footnote-78). А.А. Богданов, интегрируя различные представления о структуре международных отношений, определял собственный подход, позволяющий рассматривать систему в рамках взаимодействия с другими системными образованиями, которые находятся во внешней среде и динамично развиваются[[78]](#footnote-79).

Соответственно, представляется возможным определить системные характеристики сотрудничества ЕС и НАТО в области обеспечения кибербезопасности в рамках трансатлантического политического пространства, которые включают не только общие функции и свойства организаций, но и региональные процессы, среди которых коллективный ответ на угрозы, гомогенизация оборонного потенциала, формирование единой политики безопасности, в том числе, и появление механизмов взаимодействия в киберсфере.

Наконец, применительно к настоящему исследованию следует рассмотреть целесообразность использования теорий европейской интеграций, в частности, институционализма. Несмотря на то, что данное концептуальное направление призвано отвечать на вопросы о причинах создания институтов и их внутренних характеристиках, институционализм используется и для анализа межорганизационных отношений и их роли в рамках поведения и процесса принятия решений акторов[[79]](#footnote-80). Традиционно институционализм делится на «старый» и «новый». В то время как старый институционализм подчеркивает формальные и узаконенные институты, новый – анализирует все формы институтов, включая неформальные, и подразделяется на исторический, социологический, дискурсивный и неоинституционализм рационального выбора[[80]](#footnote-81). В случае исследования отношений ЕС и НАТО, наиболее подходящим представляется неоинституционализм рационального выбора, основанный на идее о том, что институты создаются только для максимизации выигрыша конкретного актора.

Теоретически институты в рамках данного подхода создаются только в том случае, если их наличие будет более выгодным, чем их отсутствие. Согласно Холлу и Тейлору, институты создаются с определенной целью, а субъекты используют институциональную структуру как инструмент получения определенной выгоды[[81]](#footnote-82). Говоря о ЕС и НАТО, созданных с точки зрения «принципалов» и «агентов», где правительства государств-членов (принципалы) делегируют часть полномочий институтам (агентам) и ожидают, что они смогут решить проблемы, с которыми сталкиваются субъекты, в частности, проблему обеспечения безопасности в киберпространстве, возникает вопрос, смогут ли субъекты гарантировать, что институты со временем не будут склоняться к постановке собственных целей или удовлетворению институциональных потребностей[[82]](#footnote-83). М.Э. Смит развивает эту идею, утверждая, что таким институтам как ЕС или НАТО доступно больше информации, и они имеют более широкий взгляд на решение существующих проблем, чем отдельные государства. Следовательно, институты, действующие в зоне своих интересов, могут влиять на своих членов как на более компетентных участников процесса принятия решений и формировать в зависимости от их целей повестку дня[[83]](#footnote-84).

А. Уорли критикует подобный подход, заявляя, что данный вид неоинституционализма не способен объяснить ценностную составляющую акторов и влияние институциональной среды на их выбор необходимых решений[[84]](#footnote-85). В соответствии с неоинституционализмом рационального выбора государства должны принимать свои решения для собственной выгоды, однако на практике их действия иррациональны – они вступают в коалиции или соглашения, которые забирают часть их полномочий, – но, при этом, согласуются с их ценностями или институциональными установками. Так, на практике, инвестиции США в европейскую безопасность в рамках НАТО нерациональны с экономической точки зрения, но в соответствии с ценностями это позволяет им оставаться лидером в рамках трансатлантического пространства.

Создание межправительственных организаций способствует решению определенного ряда проблем, однако нет никакой уверенности, что подобная структура не установит собственную повестку дня и не откажется от вопросов, которые изначально было поручено решить[[85]](#footnote-86). В случае сотрудничества ЕС и НАТО нет гарантии, что организации не поддержат сотрудничество в целях общей кибербезопасности, балансируя свои подходы или склоняясь к одной из организаций, учитывая разрыв между ценностями и целями стран-членов. Именно поэтому для того, чтобы учитывать возможные различия подходов ЕС и НАТО к политике кибербезопасности и оценки возможного сотрудничества или создания общего формального или неформального института сотрудничества в рамках неоинституционализма рационального выбора, следует сравнить интересы, цели и задачи, ресурсы организаций в отношении присоединения к сотрудничеству, а также определить проблемы, которые могут помешать процессу сближения. Важно оценить взаимодополняемость обеих структур в политике кибербезопасности; правила и основные направления сотрудничества. Хотя Э. Хаас явно исключал возможность «перетекания» от экономического сотрудничества к сотрудничеству в области безопасности, киберпространство может стать исключением из правила, поскольку в рамках ЕС уже наблюдается подобный процесс.

Таким образом, в связи с необходимостью проведения комплексного анализа взаимоотношений ЕС и НАТО в сфере кибербезопасности с целью выявления основных проблем, препятствующих построению устойчивых связей, и определения перспектив развития сотрудничества, представляется методологически эффективным обратиться к междисциплинарному подходу для изучения проблематики взаимодействия двух структур, включающему как общетеоретические концепции исследования международных отношений, так и теории европейской интеграции.

**Выводы к главе.** Понятие «кибербезопасность» имеет неопределённый характер. С одной стороны, оно представляется субъективным из-за его интерпретации как средства оказания влияния на пользователей сети Интернет. С другой стороны, если обратить внимание прежде всего на технологические аспекты, можно выявить его объективные стороны. В настоящем исследовании термин «кибербезопасность» будет пониматься как совокупность технологий, процессов, практик и мер реагирования, предназначенных для защиты информационно-коммуникационных систем, в том числе компьютеров, программ и данных, от повреждения, несанкционированного использования и модификации с целью обеспечения их конфиденциальности и целостности.

Вопросы обеспечения кибербезопасности приобретают международное значение, поэтому различные акторы стремятся выстроить взаимодействие таким образом, чтобы защитить собственные интересы в информационном пространстве. В частности, ЕС и НАТО наращивают собственный потенциал и продолжают сотрудничество в области безопасности и обороны, а также в сфере защиты критической инфраструктуры от кибератак. Исследованию взаимодействия ЕС и НАТО по вопросам кибербезопасности посвящено не так много научных работ, поэтому в рамках настоящего исследования планируется провести комплексный анализ аспектов сотрудничества двух организаций, подходов акторов к политике кибербезопасности, а также выявить проблемы и перспективы расширения отношений в данной сфере. С этой целью были использованы сразу несколько теоретических направлений: пространственный подход, который позволил идентифицировать трансатлантическое пространство безопасности как одну из форм транснационального политического пространства; системный подход, благодаря которому сотрудничество ЕС и НАТО будет рассмотрено как система взаимосвязи двух акторов, а также проведен сравнительный анализ подходов организаций к политике кибербезопасности; и, наконец, неоинституционализм рационального выбора, который позволит подтвердить одну из поставленных автором научных гипотез и поможет выявить основные цели, задачи и ресурсы организаций.

# **ГЛАВА 2. ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ В СТРАТЕГИЯХ ЕС И НАТО: ОБЩИЕ ЧЕРТЫ И ОСОБЕННОСТИ**

ЕС и НАТО являются одними из мировых лидеров в области обеспечения кибербезопасности и защиты критической инфраструктуры. Раннее уже было сказано о том, что организации имеют общие цели обеспечения стабильности и мира в регионе, действуют в рамках одного трансатлантического пространства и обладают схожими ценностями. Однако, некоторые элементы и практики реализации политики кибербезопасности все же могут различаться в зависимости от средств, ресурсов и инструментов, которые есть в арсенале ЕС и НАТО. Далее будут рассмотрены и проанализированы стратегии обеих организаций в области защиты киберпространства и его инфраструктуры, а также определены их основные сходства и различия.

## **2.1. Подход ЕС к политике кибербезопасности**

Изначально Европейский Союз являлся организацией, отвечающей только за экономическое развитие стран-членов. Тема безопасности только в последние несколько лет начала появляться в повестке деятельности Союза, поскольку изменения, происходящие в регионе, и возникновение новых угроз касаются в том числе и экономических аспектов развития государств. Сегодня ЕС стремится к лидерству в своей внешнеполитической и внутриполитической деятельности, включающей защиту киберпространства, условия которого меняют представление об организации.

Для защиты своей инфраструктуры от угроз, которые скрывает в себе киберпространство, ЕС предпринял множество контрмер. Первый шагом стало создание в 2004 году Европейского агентства по сетевой и информационной безопасности (ENISA)[[86]](#footnote-87), первоначальной целью которого был обмен информацией и удачными практиками защиты киберпространства между странами-членами. Однако, после хакерских атак на сайты государственных учреждений Эстонии в 2007 году встал серьезный вопрос о пересмотре собственного подхода к обеспечению кибербезопасности.

Как следствие, в 2010 году ЕС разработал «Цифровую повестку дня для Европы»[[87]](#footnote-88) и Стратегию «Европа 2020»[[88]](#footnote-89), а еще через год, признав, что киберпространство способно оказывать негативное воздействие на европейские структуры и имеет трансграничный характер, ЕС занялся разработкой внутренних стратегий в области информационной политики, а также общеевропейских руководящих принципов для обеспечения устойчивости Интернета[[89]](#footnote-90). На этом же этапе развития политики кибербезопасности ЕС определил важность наличия глобальных партнеров для решения проблем и борьбы с киберугрозами как в военном, так и в рамках гражданского измерения[[90]](#footnote-91).

2013 стал годом принятия Стратегии кибербезопасности ЕС[[91]](#footnote-92). С тех пор началось интенсивное развитие информационной политики Союза во всех ее измерениях: цифровая экономика, сетевая и информационная безопасность, борьба с киберпреступностью, а также внешняя политика и политика безопасности в области киберзащиты. Стратегия способствовала укреплению сотрудничества не только на уровне стран-членов, но и с внешними партнерами, среди которых числился НАТО. С 2015 года киберпреступность стала одним из трех столпов Европейской повестки в области безопасности[[92]](#footnote-93), а кибербезопасность – ключевым вопросом политических приоритетов, – особенно после ее включения в Стратегию цифрового рынка[[93]](#footnote-94). В 2016 год ознаменовался расширением стандартных мер ЕС по борьбе с киберугрозами, что привело к принятию Сообщения об укреплении киберустойчивой системы Европы и созданию конкурентоспособной и инновационной индустрии кибербезопасности[[94]](#footnote-95), а также Директивы по повышению безопасности сетей и информационных систем (NIS).

Директива NIS является основным правовым документом в области кибербезопасности ЕС. После ее принятия 6 июля 2016 года государствам-членам было отведено чуть меньше двух лет (21 месяц), чтобы интегрировать документ с свое национальное законодательство. В основе Директивы три основных направления деятельности государств-членов и институтов ЕС в области кибербезопасности[[95]](#footnote-96).

В соответствии с первым направлением страны-члены ЕС должны быть надлежащим образом оснащены для защиты от кибератак с помощью Компьютерной группы реагирования на чрезвычайные ситуации (CSIRT) и компетентных национальных учреждений. Второе положение предполагает сотрудничество и обмен информацией между государствами-членами ЕС. В рамках Директивы предполагалось создать единую Группу сотрудничества, чтобы облегчить процесс коммуникации. Последний приоритет предназначен для общества и экономики ЕС и призывает все государственные и частные субъекты, такие, например, как поставщики критически важной инфраструктуры, а именно связи, энергетики, транспорта, здравоохранения и финансов, а также поставщики цифровых услуг (поисковых систем, облачных сервисов, онлайн-рынков), предпринимать соответствующие меры безопасности и уведомлять национальные органы власти обо всех видах кибератак. Помимо Директивы NIS, в ЕС действует еще три законодательных акта, направленных на борьбу с киберпреступностью: Рамочное соглашение по борьбе с мошенничеством и подделкой безналичных платежных средств[[96]](#footnote-97) (2001 г.), Директива о борьбе с сексуальной эксплуатацией детей в Интернете и детской порнографией[[97]](#footnote-98) (2011 г.), Директива об атаках на информационные системы (2013 г.)[[98]](#footnote-99).

В 2016 году ЕС принял Глобальную стратегию по внешней политике и политике безопасности[[99]](#footnote-100), в которой в разделе об укреплении внутренних и внешних взаимосвязей в качестве приоритетного направления взаимодействия указывалось обеспечение кибербезопасности, а также был сделан акцент на возникновении угроз нового типа в рамках информационного пространства. В июне 2017 года Совет ЕС разработал «Инструментарий в области кибердипломатии»[[100]](#footnote-101), согласно которому одним из ключевых принципов реализации цифровой дипломатии для стран-членов ЕС стало «принятие во внимание контекста внешних отношений ЕС с заинтересованным государством». Данный набор инструментов был призван способствовать предотвращению конфликтов в киберпространстве и, как следствие, обеспечению стабильности и сотрудничества в рамках международных отношений. Наконец, в сентябре того же года Европейская комиссия и Верховный представитель Союза по иностранным делам и политике безопасности разработали свои предложения по новой киберстратегии под названием «Устойчивость, сдерживание и оборона: создание надежной политики кибербезопасности ЕС»[[101]](#footnote-102). В данном документе было предложено реформировать политику информационной безопасности ЕС на основе трех предлагаемых инициатив: создание более сильного европейского агентства в области информационной политики; внедрение общеевропейской системы сертификации кибербезопасности и оперативное внедрение Директивы NIS. Кроме того, была высказана идея создания Фонда по реагированию на чрезвычайные ситуации в области кибербезопасности, который бы мог дополнить существующие механизмы управления кризисами, что позволило бы государствам-членам получить дополнительную помощь в борьбе с серьезными угрозами.

В целом, в настоящее время данные инициативы практически реализованы, а также дополнены другими действиями ЕС в сфере киберзащиты. 16 декабря 2020 года была принята новая Стратегия кибербезопасности ЕС[[102]](#footnote-103), которая направлена на повышение устойчивости к киберугрозам и обеспечения доступа европейских граждан к надежным цифровым технологиям. Вступившая в силу Стратегия предлагает объединить деятельность и ресурсы ЕС в четырех направлениях информационной безопасности: внутреннем рынке, правоохранительных органах, дипломатии и обороне. Основой для создания документа стали План Европейской Комиссии по восстановлению Европы (NewGenerationEU), Стратегия Союза безопасности на 2020-2025 гг., и один из приоритетов Европейской комиссии на 2019-2022 гг. под названием «Европа для цифровой эпохи»[[103]](#footnote-104), который определяет следующие цели ЕС в области политики кибербезопасности:

1. Достижение устойчивости, технологического суверенитета и лидерства для того, чтобы устанавливать собственные стандарты, а не следовать правилам других государств;

2. Наращивание потенциала для предотвращения киберугроз и оперативного реагирования на подобные вызовы;

3. Расширение сотрудничества с внешними партнерами, в том числе, с другими международными союзами, для развития глобального и открытого киберпространства.

Кроме того, в рамках принятия Стратегии Комиссия внесла ряд предложений по обеспечению кибер- и физической устойчивости критически важных объектов инфраструктуры и сетей, а именно предложение о пересмотре Директивы NIS и создании NIS2, а также новой Директивы об устойчивости критической инфраструктуры.

В настоящее время деятельность ЕС по проведению политики кибербезопасности можно систематизировать следующим образом:

1. Первостепенную роль в европейской информационной политике играет Агентство по сетевой и информационной безопасности, которое занимается оперативным обнаружением, анализом и предотвращением киберинцидентов. Правовая основа ENISA – это Регламент (ЕС) 2019/881 (Закон о кибербезопасности) об ENISA и о сертификации[[104]](#footnote-105). Данный документ, принятый 17 апреля 2019 года, усилил роль Агентства в рамках наращивания сотрудничества на уровне ЕС и помощи государствам-членам, которые намерены бороться с киберугрозами[[105]](#footnote-106). Более того, Закон ввел общеевропейскую систему сертификации для товаров, услуг и процессов в рамках ИКТ, и, хотя данная инициатива все еще находится на стадии принятия, уже была создана Европейская группа по сертификации кибербезопасности (ECCG)[[106]](#footnote-107), которая помогает Комиссии и Агентству в реализации данного направления. В рамах ENISA существует Группа сертификации заинтересованных сторон по кибербезопасности (SCCG), которая также помогает основным институтам в подготовке текущей рабочей программы по данному вопросу.

2. Сотрудничеству между сообществом кибербезопасности в различных областях экономики способствует деятельность Центра обмена и анализа информации (ISAC). Дальнейшее развитие Центра как на уровне ЕС, так и на национальном уровне государств-членов является приоритетом для Европейской Комиссии.

3. Объединенный исследовательский центр (JRC) Еврокомиссии активно способствует реализации политики кибербезопасности. Например, Центром был разработан ресурс для систематизации терминологии и процессов, происходящих, в области информационной политики, что сегодня дает возможность получить более четкое представление о возможностях киберзащиты в рамках ЕС.

4. В соответствии с Директивой о безопасности сетей и информационных систем, которая была принята всеми членами ЕС, государства обязаны обеспечить наличие эффективно функционирующих Компьютерных групп реагирования на чрезвычайные ситуации (CSIRT) и Компьютерных команд быстрого реагирования (CERT). Эти структуры сотрудничают друг с другом на уровне ЕС, а также работают с частным сектором для выполнения следующих задач: мониторинг инцидентов на национальном уровне; выполнение превентивных действий; оперативное реагирование на киберугрозы; и, наконец, обеспечение анализа динамично развивающейся системы кибербезопасности, а также ситуационной осведомленности.

5. В качестве помощника Комиссии в рамках договорного государственно-частного партнерства (contractual public-private partnership) действует Европейская организация по кибербезопасности (ECSO). Большинство из 250 членов организации являются представителями индустрии информационных технологий или исследовательских учреждений. ESCO занималась разработкой рекомендаций для Horizon 2020 и его преемника Horizon Europe. В рамках первой были разработаны положения, финансируемые Комиссией и касающиеся использования кибердиапазонов и моделирования, включения малых и средних предприятий в политику кибербезопасности, обеспечения безопасности электроэнергетических систем в киберсфере, а также защиты данных и критической инфраструктуры[[107]](#footnote-108). Более того, программа Horizon 2020 предполагала создание платформы динамического управления мультиоблачными приложениями (CyCLONe), которая направлена на поставщиков подобных услуг и улучшает сквозную безопасность и сетевое управление[[108]](#footnote-109).

6. В 2017 году было создано Постоянное структурированное сотрудничество по вопросам безопасности и обороны (PESCO), являющееся частью общей политики безопасности и обороны ЕС. Целью сотрудничества выступает интеграция вооруженных сил через инструменты финансирования ряда инициатив государствами-членами. Шесть членов PESCO при руководстве Литвы с 2017 года реализуют инициативу по созданию кибергруппы быстрого реагирования и оказания взаимопомощи для обеспечения кибернетической безопасности[[109]](#footnote-110). Многие критики определяют данную структуру как дублирование или конкуренцию деятельности НАТО, однако в ЕС заявляют, что это является лишь дополнением к действиям военно-политического альянса, поскольку не все страны-члены ЕС являются союзниками по НАТО. Более того, генеральный секретарь Йенс Столтенберг также заявил, что создание программы сотрудничества PESCO только «укрепит европейский столп внутри НАТО»[[110]](#footnote-111).

7. Для усиления реагирования правоохранительных органов на киберпреступность в ЕС и защиты европейских граждан, предприятий и правительств от онлайн-преступлений Европолом в 2013 году был создан Европейский центр по борьбе с киберпреступностью. Основная роль EC3 заключается в борьбе с трансграничными кибератаками. Являясь центром информации о преступлениях и разведданных, EC3 оказывает всевозможную помощь в киберзащите и предоставляет государствам-членам специализированных технических экспертов-криминалистов для проведения расследований и киберопераций[[111]](#footnote-112). В рамках EC3 в 2014 году была создана Совместная группа по борьбе с киберпреступностью (J-CAT), которая несет ответственность за обеспечение скоординированных действий на основе разведданных о киберугрозах для содействия совместному выявлению и проведению расследований и операций с внешними партнерами[[112]](#footnote-113). В 2019 году Европол объявил о принятии нового Протокола экстренного реагирования правоохранительных органов ЕС на крупные трансграничные кибератаки, реализация которого возложена на Европейский центр по борьбе с киберпреступностью[[113]](#footnote-114).

Говоря о планах ЕС в области обеспечения кибербезопасности, также можно выделить несколько направлений. Во-первых, в декабре 2020 года было Комиссией было внесено предложение об устранении недостатков предыдущей Директивы NIS и создании новой. Данное предложение должно расширить сферу действия Директивы за счет добавления новых секторов в зависимости от их важности для экономики и общества. Кроме того, предложение ужесточает требования к безопасности для компаний, вводя более точные положения о процессе информирования об инцидентах, содержании отчетов и сроках. Оно устанавливает базовую структуру с ответственными ключевыми субъектами для скоординированной деятельности и оперативного обнаружения уязвимостей на основе реестра ЕС и ENISA[[114]](#footnote-115).

Во-вторых, 23 июня 2021 года президентом Еврокомиссии Урсулой фон дер Ляйен была выдвинута рекомендация о создании Объединенного киберподразделения, что стало бы важным шагом на пути к завершению формирования европейской системы управления кризисными ситуациями в киберпространстве. Сегодня уже существуют «киберполигоны», создание которых финансируется в рамках Horizon 2020, Horizon Europe и программы Digital Europe, представляющие собой среду для моделирования киберугроз в рамах обучения специалистов.

Наконец, Европейский центр промышленной, технологической и исследовательской квалификации в области кибербезопасности собирается объединить имеющийся опыт и координировать разработку и внедрение новейших технологий в сфере киберзащиты. В частности, в рамках этого проекта уже разработана комплексная платформа под названием «Атлас безопасности», которая помогает в управлении знаниями для картирования, классификации и стимулирования сотрудничества в поддержку цифровой стратегии ЕС.

Таким образом, на основе вышеизложенных данных представляется возможным определить институциональные рамки ЕС[[115]](#footnote-116) и основные характеристики европейского подхода в области обеспечения политики кибербезопасности. Таковыми являются три направления информационной политики. Во-первых, повышение безопасности сетевых и информационных систем, включая определение высоких стандартов для всех объектов, разработку европейской киберзащиты для обнаружения уязвимостей и превентивных мер, поддержку малого и среднего бизнеса, привлечение специалистов в области кибербезопасности и инвестиции в исследования и инновации. Во-вторых, укрепление коллективных возможностей для оперативного реагирования на кибератаки, в том числе поддержка государств-членов в защите своих граждан и интересов национальной безопасности, совместная работа по реализации задач политики кибербезопасности, обеспечение эффективного функционирования правоохранительных органов и судебной системы, а также осуществление кибердипломатии и создание объединенного киберподразделения. Наконец, работа с внешними партнерами для обеспечения международной безопасности и стабильности в киберпространстве, а также продвижения глобального, открытого и безопасного Интернета, в котором соблюдаются международное право, права человека, основные свободы и демократические ценности.

## **2.2. Подход НАТО к политике кибербезопасности**

Североатлантический Альянс стал первой международной организацией, которая обратила внимание на важность киберзащиты. Начало политики кибербезопасности в НАТО было положено 1999 году, когда Альянс подвергся атаке хактивистов во время операции «Союзные силы» в Югославии[[116]](#footnote-117). После этого инцидента военно-политический союз определил необходимость ведения политики кибербезопасности и включил ее в политическую повестку дня, сосредоточившись на разработке собственной стратегии. Спустя три года на саммите в Праге была утверждена Программа киберзащиты[[117]](#footnote-118) и создано средство быстрого реагирования для предотвращения и обнаружения уязвимостей в киберпространстве, а именно Технический центр по реагированию на компьютерные инциденты (NCIRC)[[118]](#footnote-119).

Кибератака на государственные учреждения в Эстонии в 2007 году не только спровоцировала решительные действия со стороны ЕС, но и оказала влияние на политику НАТО, в рамках которого встал вопрос о создании законодательства о действиях и процессах принятия решений в области нового измерения – киберпространства. В 2008 году на Бухарестском саммите была принята первая политика НАТО в области киберзащиты, в которой подчеркивалась необходимость защиты ключевых информационных систем организации и государств-членов, обмена передовым опытом и предоставления возможностей для оказания помощи странам-союзникам по запросу в противодействии кибератакам[[119]](#footnote-120).

Следующим шагом стало создание двух институтов киберзащиты. В 2008 году был создан Центр управления кибервойной НАТО (CDMA), цель которого управлять и координировать киберзащиту союзников, а также помогать государствам-членам улучшать национальные оперативные возможности[[120]](#footnote-121). В Эстонии располагается другое учреждение – Центр передового опыта по совместной киберзащите (CCD COE), – миссия которого заключается в укреплении потенциала и сотрудничества, стимулировании обмена информацией между НАТО и странами-партнерами через образование, исследования и консультации[[121]](#footnote-122).

Лиссабонский саммит 2010 года ознаменовался принятием Стратегической концепции НАТО[[122]](#footnote-123), которая включала и кибербезопасность. В рамках саммита был также принят Лиссабонский пакет возможностей[[123]](#footnote-124), целью которого стало оказание помощи государствам-членам в обнаружении, оценке, предотвращении, защите и восстановлении после злонамеренных действий, и который включал План действий в области киберзащиты. Аналогичный документ был одобрен в 2014 году на Уэльском саммите[[124]](#footnote-125).

В рамках Варшавского саммита союзники по НАТО договорились продолжить действия по киберзащите национальных инфраструктур и сетей посредством Обязательства по киберзащите[[125]](#footnote-126). Государства-члены согласились с тем, что киберпространство должно быть приравнено к оперативной области так же, как и другие пространства, которые могут быть подвержены угрозам (суша, вода, воздух, космос). В 2017 году План киберзащиты был дополнен дорожной картой[[126]](#footnote-127).

Таллиннское руководство по международному праву, применимому к кибернетическим войнам (Tallinn Manual), которое было подготовлено Центром передового опыта по совместной киберзащите и опубликовано в двух изданиях (2013 и 2017 гг.), стало основополагающим нормативно-правовым документом НАТО в сфере кибербезопасности. В документах содержится анализ действующего законодательства, касающегося jus ad bellum и jus in bello (где первое – это право прибегать к войне и, в общем, к силе, а второе – это право, регулирующее поведение воюющих сторон во время вооруженного конфликта), и подтверждающего, что регулирование действий государств в киберпространстве зависит от международного права[[127]](#footnote-128). Tallinn 2.0 содержит руководящие принципы о том, как государства могут определять правила ведения боевых действий, контрмеры, операции возмездия и другие формы реагирования в контексте международного права, если им предстоит столкнуться с актом кибератаки.

В 2018 году на саммите в Брюсселе лидеры стран Альянса договорились о создании нового Центра операций в киберпространстве в рамках усиленной структуры органов военного управления НАТО, а также условились, что организация может использовать национальные кибернетические возможности для проведения своих операций и миссий, при этом, союзники сохраняют в собственности данную инфраструктуру или иные инструменты так же, как и владеют на сегодняшний день танками, кораблями и самолетами.

На саммите НАТО в Брюсселе в 2021 году государства-члены одобрили новую Комплексную политику киберзащиты, которая определила три основные задачи НАТО по коллективной обороне, урегулированию кризисов и укреплению безопасности на уровне сотрудничества. В сентябре того же года в НАТО был назначен первый директор по информационным технологиям для содействия интеграции, согласованию и сплочению систем ИКТ в масштабах всего военно-политического блока, который относится к Агентству НАТО по обеспечению и закупкам. В апреле 2022 года союзники и партнеры по НАТО приняли участие в масштабных киберучениях Locked Shields, в которых Финляндия была объявлена победителем, а второе и третье место разделили литовско-польская и эстонская группа соответственно[[128]](#footnote-129).

В настоящее время деятельность НАТО в области осуществления политики кибербезопасности можно систематизировать следующим образом:

1. Технический центр по реагированию на компьютерные инциденты (NCIRC), базирующийся в SHAPE в Монсе, защищает собственные сети НАТО, обеспечивая централизованную и круглосуточную поддержку киберзащиты. Альянсом также был создан Центр киберопераций в Монсе, который занимается информированием об операциях и миссиях НАТО, а также координирует оперативную деятельность организации в киберпространстве, обеспечивая свободу действий в этой области и делая операции более устойчивыми к киберугрозам. Деятельность NCIRC тесно связана с Группами быстрого реагирования (RRTs), которые включают 200 экспертов из всех стран Альянса и обеспечивают постоянную поддержку киберзащиты компьютерной сети Альянса[[129]](#footnote-130).

2. Агентство связи и информации НАТО (NCIA) было создано в 2012 году посредством слияния нескольких учреждений: Агентства НАТО по консультациям, командованию и управлению (NC3A), Агентства служб связи и информационных систем НАТО (NCSA), Агентства управления воздушным командованием и системой управления НАТО (NACMA) и Службы информационных и коммуникационных технологий штаб-квартиры НАТО (ICTM). Агентство предоставляет специализированные услуги по предотвращению, обнаружению, реагированию и восстановлению после инцидентов в киберпространстве, а также выступает в качестве центра обмена киберинформацией и обучения для союзников и государств-партнеров. 12 февраля 2019 года Агентство предприняло первый шаг к запуску защищенной бизнес-сети НАТО, которая обеспечивает рабочее пространство для допуска к безопасным Интернет-продуктам[[130]](#footnote-131).

3. Центр передового опыта по совместной киберзащите (CCD CE) находится в Таллинне и, в отличие от других учреждений, не входит в Командную структуру НАТО, поскольку основной целью института является предоставление опыта в области кибезащиты. В последнее время CCD CE активно оказывает правовую поддержку в рамках Альянса: уже было выпущено два издания Таллиннского руководства, организованы совместные учения под названием Cyber Coalition для проверки кибернетической готовности государств-членов[[131]](#footnote-132). В Эстонии также находится Киберполигон НАТО (Cyber Range), который используется для проведения ежегодных флагманских учений и тренировок, включая учения по управлению кризисными ситуациями. Его управление осуществляется Силами обороны Эстонии. Более того, у НАТО есть ряд практических инструментов для повышения осведомленности государств-членов. В Меморандуме о взаимопонимании[[132]](#footnote-133) изложены механизмы обмена информацией и помощи в улучшении национальных инструментов реагирования на подобные инциденты. Обмен технической информацией также осуществляется через Платформу обмена информацией о вредоносных программах[[133]](#footnote-134), которая была разработана в ноябре 2013 года.

4. На территории Германии, в баварской деревне Обераммергау, располагается Школа НАТО, которая проводит обучение по кибербезопасности для поддержки операций, стратегий, политики и процедур НАТО. Образовательные программы также проводятся Академией связи и информации НАТО в Оэйраше (Португалия) и Оборонным колледжем в Риме (Италия)[[134]](#footnote-135).

5. Частный сектор является ключевым игроком в киберпространстве, поэтому альянсом было создано Промышленное киберпартнерство, союзники которого работают над укреплением своих отношений с представителями промышленности и академическими кругами и входят в подразделения НАТО и национальные компьютерные группы реагирования на чрезвычайные ситуации (CERT).

Будущее развитие НАТО, в том числе в области киберзащиты, определяется рекомендациями и предложениями, которые были выдвинуты независимой аналитической группой, назначенной Генеральным Секретарем НАТО на встрече в Лондоне в декабре 2019 года, в рамках программы «НАТО 2030». Йенс Столтенберг поручил подготовить рекомендации в трех областях:

1. Укрепление единства, солидарности и сплоченности союзников для усиления центральной роли трансатлантических связей;

2. Расширение политических консультаций и координации между союзниками по НАТО;

3. Усиление политической роли НАТО и соответствующих инструментов для противодействия текущим и будущим угрозам и вызовам Североатлантического Альянса[[135]](#footnote-136).

В итоге был составлен документ, который призван информировать Генерального Секретаря об обсуждениях в рамках выработки рекомендаций будущего развития НАТО. По словам группы независимых экспертов, гибридные вызовы и кибератаки сами по себе не являются угрозами, а только представляют инструменты, используемые враждебными субъектами, которые преследуют стратегическую цель, заключающуюся в подрыве международного порядка и демократических систем управления, а также ослаблении НАТО. В связи с этим были предложены следующие меры для усиления роли НАТО:

* Необходимо следовать Докладу об усилении мер реагирования НАТО на гибридные угрозы, что поможет бороться с нынешней фрагментацией мнений по вопросам обеспечения безопасности внутри структур НАТО.
* Опираясь на результаты Брюссельского саммита, Альянсу следует укрепить свой потенциал по поддержке союзников в защите от гибридных угроз и кибератак (согласно статье 5), а также чаще обращаться к формату консультаций для политического диалога и демонстрации единства (согласно статье 4).
* Следует повышать осведомленность о природе происхождения гибридных угроз и организованных преступных групп, стоящих за ними. Она должна включать общую терминологию и владение ситуационной информацией, чего можно добиться посредством обнаружения, мониторинга и анализа гибридных угроз, прогнозных исследований, обмена передовым опытом, сценарных игр в рамках киберучений[[136]](#footnote-137).
* НАТО и государства-партнеры должны создавать больше возможностей для действий в виртуальном измерении, в том числе на тактическом уровне. Эти возможности необходимы для обнаружения дезинформации и оказания поддержки в предотвращении или ограничении ее воздействия путем повышения осведомленности граждан. Одновременно НАТО и союзникам необходимо создать правовые и этические рамки, чтобы иметь возможность эффективно и законно действовать в этих измерениях.
* НАТО следует периодически отрабатывать варианты реагирования на гибридные угрозы, основанные на реалистичных сценариях, в максимально тесном сотрудничестве с субъектами, представляющими дипломатические, информационные, военные, экономические, финансовые, разведывательные и правоохранительные инструменты. Эти тренировки и учения должны разрабатываться как на тактически-оперативном, так и на политико-стратегическом уровне.
* Необходимо иметь возможность финансировать, увеличивать и обучать персонал новейшим способам киберзащиты, а также обеспечивать наличие необходимой политической и правовой базы для решения настоящих и будущих проблем в этих сферах[[137]](#footnote-138).

В рамках Брюссельского саммита 14 июня 2021 года и принятого по итогам встречи Коммюнике была признана особая роль киберзащиты. Страны-союзники согласились шире использовать площадку НАТО для политических консультаций и обмена национальными подходами и опытом. Кроме того, было обещано интегрировать национальные практики в коллективную оборону, операции и миссии Альянса, стремиться к развитию взаимовыгодных и эффективных партнерских отношений со странами-партнерами, международными организациями, промышленностью и академическим сообществом, способствуя усилиям по укреплению международной стабильности в киберпространстве[[138]](#footnote-139).

Таким образом, на основе анализа деятельности НАТО в области киберзащиты, также представляется возможным, как и для ЕС, определить ее институциональную структуру[[139]](#footnote-140), а также выделить основные принципы в подходе военно-политического блока к политике кибербезопасности. Во-первых, государства-члены НАТО признают киберпространство такой же областью проведения операций как вода, суша, воздух и космос. С этой целью НАТО адаптирует свои программы обучения и подготовки к киберсфере. Во-вторых, союзники по НАТО приняли Обязательства по киберзащите, согласно которым обязаны поддерживать и развивать свою индивидуальную коллективную способность противостоять киберугрозам. Наконец, НАТО приветствует тесное сотрудничество с постоянно растущим кругом партнеров. Одним из таких является Европейский Союз, с которым Альянс ежегодно расширяет связи, особенно в таких областях как обмен информацией, обучение, совместные исследования и учения.

**Выводы к главе.** ЕС и НАТО одинаково определяют важность реализации политики кибербезопасности, предпринимают соответствующие меры для ее укрепления и развития и приветствуют международное сотрудничество как необходимость в создании глобального и безопасного информационного пространства. Возвращаясь к теории секьюритизации, следует определить основные характеристики угроз, представляющих особое значение для ЕС и НАТО, а также референтные объекты, на которые могут быть направлены подобные вызовы. В первом случае, можно отметить идентичные характерные черты опасностей, которым организации отдают приоритет в рамках своей политики кибербезопасности. В основном, такие вызовы для критической инфраструктуры и информационного пространства исходят от конкретных государств или национальных преступных группировок. При этом, референтные объекты разнятся в зависимости от целей и задач организаций: ЕС в своей деятельности уделяет внимание безопасности государств-членов, тогда как НАТО акцентирует свои действия на защите собственной инфраструктуры и информационного пространства.

Благодаря сравнительному анализу[[140]](#footnote-141) подходов организаций удалось вывить общие черты и индивидуальные особенности каждой в сфере обеспечения кибербезопасности.

К общим чертам следует отнести:

* Наличие постоянно действующей нормативно-правовой базы, которая включает общий подход организаций к политике кибербезопасности, основные инструменты и формы деятельности, реализуемые в рамках обеспечения эффективной защиты кибернетической инфраструктуры и процессов. Обе организации имеют профильные стратегические документы;
* Широкий ряд институтов и инструментов, которые задействованы в осуществлении политики кибербезопасности. ЕС и НАТО имеют основные и второстепенные институты, отвечающие за различные направления деятельности структур в сфере киберзащиты. Более того, организации имеют институты, отвечающие за реализацию политики кибербезопасности в рамках государств-членов, в частности Компьютерные группы реагирования на чрезвычайные ситуации и Компьютерные команды быстрого реагирования;
* Цели ЕС и НАТО, которые совпадают по нескольким направлениям: 1) повышение осведомленности; 2) защита национальных интересов и интересов организаций в киберпространстве; 3) укрепление единства государств-членов; 4) тесное сотрудничество с внешними партнерами, в том числе, с другими международными организациями;
* Похожие действия, которые организации предпринимают для защиты кибернетической инфраструктуры и процессов: 1) проведение исследований и международных программ обучения; 2) финансирование перспективных проектов и создание фондов в этих целях; 3) помощь государствам-членам в борьбе с киберугрозами и их последствиями;
* Ряд общих целей в рамках перспектив развития ЕС и НАТО: 1) расширение программы проведения киберучений и увеличение числа специалистов в области кибербезопасности; 2) укрепление потенциала сотрудников через объединение имеющегося опыта и повышение технологических стандартов; 3) дальнейшее расширение или обновление нормативно-правовой базы в области кибербезопасности.

Основными особенностями в реализации политики кибербезопасности ЕС и НАТО выступают следующие положения:

* В НАТО в большей степени представлены институты, которые осуществляют международное обучение для реализации политики кибербезопасности. В ЕС этими задачами частично занимаются центры обмена информацией и исследовательские центры, которые профилированы создавать инновационные продукты и повышать осведомленность государств-членов;
* В НАТО больше развита система киберучений, а также существует постоянный киберполигон, который позволяет союзникам и партнерам моделировать ситуации киберугроз и решать их. ЕС условно заявляет о наличии таких возможностей, но на постоянной основе не проводит киберучения, как, например, в случае с ежегодными флагманскими учениями НАТО Cyber Coalition;
* НАТО в отличие от ЕС большую роль уделяет сотрудничеству с внешним кругом партнеров, определяя эту цель приоритетом политики кибербезопасности. ЕС в стратегических и иных профильных документах больше ссылается на достижение автономии в вопросах безопасности, хотя и упоминает сотрудничество с партнерами;
* ЕС имеет больше опыта в создании фондов для финансирования перспективных проектов в сфере кибербезопасности. НАТО включает данный вопрос в общую повестку по обеспечению безопасности.

Таким образом, ЕС и НАТО имеют как общие, так и уникальные черты в реализации политики кибербезопасности в рамках трансатлантического пространства, которые могут не только быть использованы в пользу расширения дальнейшего сотрудничества благодаря поиску общих целей и задач, но и помешать выстраиванию эффективного взаимодействия.

# **ГЛАВА 3. СОТРУДНИЧЕСТВО ЕС И НАТО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ**

## **3.1. Взаимодействие НАТО и ЕС в сфере кибербезопасности на современном этапе:** **институционально-правовые аспекты и текущие проблемы**

В начале 2001 года ЕС и НАТО определили друг друга в качестве стратегических партнеров в области безопасности. Позже в рамках Лиссабонского саммита 2010 года организации признали необходимость сотрудничества в рамках управления кризисами[[141]](#footnote-142). Основой для начала более тесного взаимодействия стала потребность в стирании границ между военным и гражданским направлениями деятельности: большинство представителей военных подразделений НАТО не обладало такими знаниями как государственное управление и политика, а сотрудничество должно было позволить членам обеих структур объединять накопленные знания и, тем самым, повышать собственный потенциал в противостоянии традиционным и гибридным угрозам[[142]](#footnote-143).

На сегодняшний день сотрудничество ЕС и НАТО необходимо для содействия эффективному и многостороннему реагированию на современные угрозы безопасности. Однако, с момента принятия Маастрихтского договора и включения широкого круга внешнеполитических вопросов в повестку ЕС, а также определения Общей внешней политики и политики безопасности, вопрос взаимодействия структур стал сложной задачей. В целом, растущая роль ЕС в международном кризисном управлении приветствовалась союзниками по НАТО с точки зрения анализа потребностей обеих организаций, но политический контекст и межведомственное соперничество не позволяли в полной мере найти компромиссы в области определения общей политики безопасности.

За последние несколько лет наметился импульс для возобновления сотрудничества. В 2016 году ЕС и НАТО приняли Совместную декларацию, которая заложила основу для нового типа отношений[[143]](#footnote-144). В тексте документа содержался призыв придать «новое содержание стратегическому партнерству ЕС-НАТО» и продолжить взаимодействие в следующих областях:

* Противодействие гибридным угрозам;
* Обеспечение морской безопасности;
* Киберзащита и оборона;
* Поддержание оборонного потенциала;
* Улучшение оборонной промышленности и научных исследований;
* Проведение совместных учений;
* Обеспечение устойчивости партнеров.

В 2018 году ЕС и НАТО подписали вторую Совместную декларацию, согласно которой сотрудничество предполагалось в четырех ключевых областях: мобильность военного персонала и инфраструктуры; борьба с терроризмом; устойчивость к химическим, биологическим, радиоактивным и ядерным рискам; а также повышение роли женщин в обеспечении мира и безопасности[[144]](#footnote-145). Государства-члены обеих структур одобрили процесс укрепления политического диалога, и не менее 74 пунктов были определены в качестве направлений сотрудничества.

Оба документа способствовали улучшению взаимодействия между ЕС и НАТО в ряде областей. Во-первых, был выстроен политический диалог между Генеральным секретарем НАТО и его заместителем с одной стороны, и Высоким представителем по иностранным делам и политике безопасности ЕС и европейскими комиссарами с другой. Присутствие Генерального секретаря НАТО и вице-президента ЕС на встречах министров обороны (или иностранных дел) другой организации стало обычной практикой. Более того, структуры начали взаимодействовать на уровне Североатлантического совета и Комитета по политике и безопасности ЕС, а также в рамках официальных и неофициальных встреч[[145]](#footnote-146).

Во-вторых, большинство подразделений или учреждений широко интегрировали в свою работу фактор сотрудничества ЕС-НАТО. Чаще стали проводиться совместные брифинги по вопросам, представляющим взаимный интерес, а представители каждого учреждения с тех пор участвуют в заседаниях организации-партнера[[146]](#footnote-147).

Наконец, обе организации добились значительного прогресса в своем сотрудничестве не только в рамках тематических направлений, как гибридные угрозы, кибербезопасность и оборона, но и на местах, когда наблюдается совместное развертывание миссий, как в случае с Ираком или в Средиземном море. Как верно отмечается в последовательных отчетах о ходе сотрудничества ЕС-НАТО, данные шаги необходимо рассматривать в долгосрочной перспективе: хотя на данный момент подобные тенденции сближения не приводят к конкретным результатам, благодаря «процессу постоянного взаимодействия» такие меры станут причиной прогресса в будущем[[147]](#footnote-148).

Одним из основных направлений сотрудничества организаций является кибербезопасность. ЕС и НАТО подвергаются одним и тем же по характеру киберугрозам, которые подрывают все сферы жизни общества, угрожая гражданской, политической, экономической и военной безопасности. Кибератаки на государственные учреждения 2007 года заставили обе организации серьезно задуматься о новом типе угроз. В 2011 году НАТО одобрил усиленную политику и план действий в области киберзащиты, а в 2016 году было принято решение о введении киберпространства в действие в рамках оборонной политики и планирования. На саммите в Брюсселе в июне 2018 года страны-члены приняли первую Стратегию по кибербезопасности. ЕС, в свою очередь, сделал борьбу с киберпреступностью одним из трех столпов Европейской повестки дня в области обеспечения безопасности и признал кибербезопасность приоритетом Глобальной стратегии по внешней политике и политике безопасности на 2016 год. Более того, в 2017 году Брюссель принял «Пакет мер по кибербезопасности», включающий пересмотренную Стратегию кибербезопасности и «Инструментарий кибердипломатии».

В подобной обстановке ЕС и НАТО стали рассматривать друг друга в качестве взаимодополняющих партнеров в стремлении повысить свою киберустойчивость. С этой целью, а также для обмена информацией на оперативном уровне в феврале 2016 года организации подписали Техническое соглашение по киберзащите между Техническим центром НАТО по реагированию на компьютерные инциденты (NCIRC) и Группой реагирования на компьютерные чрезвычайные ситуации ЕС (CERT-EU). Наиболее значительный вклад был сделан благодаря подписанию двух упомянутых раннее Совместных деклараций, которые создали институционально-правовые рамки сотрудничества структур в рамках безопасности и обороны[[148]](#footnote-149).

В 2017 году Эстония, председательствующая в Совете Европейского Союза, созвала флагманскую конференцию, чтобы стимулировать развитие нового мышления в отношении сотрудничества ЕС–НАТО в области кибербезопасности и обороны. В результате для содействия обмену передовыми практиками в области противостояния киберугрозам и предотвращения их последствий, а также управления кризисами и реагирования на них был определен общий набор предложений в рамках кибернетического сотрудничества[[149]](#footnote-150).

С тех пор активное взаимодействие в области кибербезопасности значительно улучшилось благодаря интенсивному и регулярному обмену информацией об учебных и образовательных курсах, перекрестным брифингам, а также ежегодному совещанию высокого уровня «Диалог между ЕС и НАТО»[[150]](#footnote-151). Кроме того, структуры занимаются анализом сотрудничества и выпускают ежегодные отчеты о проделанной работе.

Еще одним достижением в рамках институционального взаимодействия является факт того, что с 2017 года флагманские учения ЕС и НАТО по управлению кризисными ситуациями (EU PACE и NATO CMX) координируются и проводятся параллельно и в присутствии военных штабов организаций, а уже в 2018 году ЕС присоединился к ежегодным учениям Locked Shields[[151]](#footnote-152).

В 2019 году в ежегодном отчете отмечалось активное взаимодействие ЕС и НАТО в сфере кибербезопасности, включающее перекрестные брифинги по вопросам Инструментария кибердипломатии ЕС и усилиям НАТО по киберзащите, а также продолжающееся сотрудничество в области образования, а именно открытие курса НАТО по кибербезопасности и совместное участие партнеров в Международной конференции по киберконфликтам 2018 года[[152]](#footnote-153). В октябре 2019 года представители ЕС приняли участие в форуме «CYBERSEC 2019», организованном Центром передового опыта контрразведки НАТО. В декабре того же года в рамках штабных переговоров высокого уровня ЕС-НАТО были проведены тематические сессии, посвященные усилиям по интеграции кибернетических аспектов в антикризисном управлении; повышению сетевой безопасности и устойчивости, включая 5G и безопасность цепочек поставок; содействию кибернетической стабильности государств-членов; и укреплению сотрудничества между соответствующими учреждениями по реагированию на инциденты в киберпространстве[[153]](#footnote-154).

В 2020-2021 годах между ЕС и НАТО продолжился обмен опытом и передовыми практиками. В мае 2021 года в качестве параллельного мероприятия в контексте учений EU Integrated Resolve 20 была организована специальная дискуссия, чтобы лучше понять и рассмотреть потенциальные возможности сотрудничества между организациями. Кроме того, военный штаб ЕС разработал концепцию «Военное видение ЕС и Стратегия в киберпространстве как области операций», которая, как ожидается, будет распространена среди сотрудников НАТО. В октябре 2020 года Проектная группа Европейского оборонного агентства (EDA) по киберзащите приняла участие в Ежегодной дисциплинарной конференции НАТО, предоставив союзникам обновленную информацию о проектах ЕС по киберобразованию и учениям[[154]](#footnote-155). Таким образом, следуя логике схематичного представления институциональной структуры реализации политики кибербезопасности для двух организации, можно составить аналогичную схему, которая будет отражать формы сотрудничества ЕС и НАТО в сфере киберзащиты[[155]](#footnote-156).

Объясняя причины установления связей ЕС и НАТО в области обеспечения политики кибербезопасности, следует обратиться к теоретическим основам исследования. Институционализм рационального выбора утверждает, что новый институт должен быть создан только в том случае, если нет другого варианта, который был бы более эффективным и использовал бы уже существующие. Следовательно, сотрудничество ЕС и НАТО было более эффективным выбором отчасти с точки зрения административных аспектов, поскольку, с одной стороны, для ЕС не нужно было создавать новую систему, так как у партнерских организаций уже есть действующая, а, с другой стороны, это сотрудничество предоставило ЕС знания, необходимые для развития в сфере безопасности и современные инструменты и методы борьбы с киберугрозами. В свою очередь, для НАТО этот шаг стал полезным в плане получения новых знаний в области государственного управления, а также поиска новых союзников из тех членов ЕС, которые не состоят в НАТО. Кроме того, сотрудничество организаций в значительной степени зависит от отношений ЕС и США, которые всегда были значительными, а для США, как известно, важно иметь свои рычаги влияния в европейском регионе[[156]](#footnote-157). Таким образом, из финансовых, административных и основанных на знаниях мотивов взаимодействия для обеих организаций стало рациональным сотрудничество в области образования, профессиональной подготовки, сбора информации и мобильности в сфере кибербезопасности. Однако, данный процесс требует от государств-членов высокого уровня доверия, так как здесь возникают вопросы совместимости между ценностями организаций и стратегическими целями[[157]](#footnote-158). В связи с этим следует обратить внимание на проблемы, которые мешают ЕС и НАТО расширять сотрудничество и интегрировать свои подходы.

Условно препятствия, которые существуют между организациями в рамках сотрудничества в области кибербезопасности, можно рассматривать в двух измерениях: на наднациональном уровне и на уровне государств-членов[[158]](#footnote-159). Полноценный совместный ответ ЕС-НАТО на киберугрозы возможен только в том случае, если обе организации имеют общую ситуационную осведомленность и восприятие угроз, основанные на общих показателях и их оценке. Это может быть достигнуто только путем регулярного обмена информацией, и, хотя взаимодействие между штабами в последнее время значительно улучшилось, тем не менее ЕС и НАТО остаются двумя отдельными организациями, каждая из которых поддерживает ограничительные процедуры обмена данными, препятствующие достижению общего понимания существующих вызовов. Кроме того, проблема во многих случаях возникает из-за разного членства. В этом случае возникает ситуация, когда руководящие органы делятся информацией только с ЕС или только с НАТО, или правительства отказываются делиться своими данными на наднациональном уровне. При этом случае если информации удается достичь, то она чаще засекречена, а непосредственных каналов для обмена секретной информацией между ЕС и НАТО еще нет. Соответственно, стандарты и практика обеспечения безопасности информации все еще различны, чтобы поддерживать доверие и традицию обмена данными.

Примером подобного недопонимания может служить ситуация, связанная со всемирной кибератакой WannaCry. Чтобы справиться с программой-вымогателем в Агентстве ЕС по сетевой и информационной безопасности (ENISA) была создана специальная целевая группа для координации региональных действий. По данным Агентства, это был «первый в истории случай киберсотрудничества на уровне ЕС», в котором для преодоления кризиса использовались стандартные операционные процедуры, установленные и обычно отрабатываемые во время учений Cyber Europe. Механизм сотрудничества ЕС был опробован во второй раз два месяца спустя во время вспышки NonPetya. Из общедоступных источников неизвестно, активировал ли НАТО какой-либо механизм реагирования во время распространения двух вредоносных программ. Тем не менее, Генеральный секретарь Йенс Столтенберг заявил, что CERT-EU и NCIRC обменивались информацией и предупреждениями в режиме реального времени[[159]](#footnote-160). Таким образом, анализируя киберполитики ЕС и НАТО, а также их ответы на соответствующие кризисы, можно заметить довольно четкое разделение труда между двумя организациями. В том время как ЕС готовится к кризисам, затрагивающим критическую инфраструктуру его государств-членов, НАТО уделяет внимание своим собственным сетям и системам. Указанные кибератаки привели в действие механизм сотрудничества ЕС, но не побудили Североатлантический совет санкционировать какой-либо коллективный ответ.

Что же касается сотрудничества на уровне государств-членов, то несмотря на все амбиции ЕС и НАТО в рамках институционального развития и интеграции на данном уровне, организации все еще зависимы от своих членов в поддержке наднационального подхода. Государства не всегда готовы идти на сотрудничество с институтами, так как кибербезопасность все еще остается важной областью национальных интересов. Более того, обеспечение передовых кибернетических решений потребовало бы от государств-членов организаций быть более прозрачными в предоставлении разведданных об угрозах и информации о киберинцидентах, но в основном они оказываются к этому не готовы. Остается неясным вопрос о том, как в будущем можно было бы повысить роль ЕС и НАТО или их сотрудничества в киберпространстве, если ряд рекомендаций, адресованных организациями своим членам, не имеют обязательный характер. Государства, нуждающиеся в повышении своей национальной устойчивости, по-прежнему скептически относятся к тому, что ЕС или НАТО предоставляют внешнюю помощь, соответствующую их национальным потребностям, и часто не желают обращаться за поддержкой на наднациональном уровне. Подобное несоответствие приводит к ситуации, когда кибернетические возможности государств становятся не совместимыми, не дополняют друг друга и не координируются.

Несмотря на вышеуказанные проблемы, ЕС и НАТО могут в будущем продолжить работать вместе. Во-первых, это приносит хоть и не большую, но пользу обеим организациям, которая заключается в усилении оборонного потенциала и повышении киберустойчивости. Во-вторых, в нынешних условиях структуры все больше приходят к пониманию того, что только совместные усилия позволят противостоять новому типу угроз. Наконец, союзники по НАТО и страны-члены ЕС в большинстве своем поддерживают данное сотрудничество, необходимо только определить общие ориентиры и выбрать правильное направление для укрепления уже существующих связей.

## **3.2. Потенциал развития сотрудничества ЕС И НАТО в сфере кибербезопасности**

Сотрудничество ЕС и НАТО на сегодняшний день имеет важное значение для того, чтобы институты и правительства в рамках трансатлантического политического пространства получили возможность оперативно выявлять и эффективно сдерживать кибератаки, а также привлекать к ответственности тех, кто в этом виновен. Обе организации должны продолжить искать новые пути взаимодействия, которые будут углублять и расширять уже сложившуюся модель сотрудничества.

Для того, чтобы определить дальнейшие перспективы развития отношений ЕС и НАТО следует учитывать ряд факторов, которые основываются на анализе прошлых тенденций взаимодействия, современной ситуации, а также индивидуальных и коллективных ожиданиях организаций, отраженных в стратегических документах. В связи с этим представляется необходимым провести качественный контент-анализ подобного рода документов, чтобы выделить основные направления, по которым ЕС и НАТО готовы сотрудничать в будущем или развивать собственный потенциал. В исследовании использован подход Б. Берельсона, в соответствии с которым определяют следующие единицы анализа: 1) понятия, выраженные в словах и сочетаниях слов; 2) темы, выраженные в предложениях, фрагментах текста (например, абзацах) или даже целостных текстах; 3) политическая ситуация или событие, рассматриваемые в целом. Согласно Б. Берельсону, целями контент-анализа могут быть описание тенденций в изменении или различий в содержании определенных процессов; определение намерений или иных характеристик участников процессов; выявление интересов, установок и ценностей участников процессов[[160]](#footnote-161). В настоящем исследовании в качестве единиц анализа будут взяты отдельные темы, а цель будет состоять в описании тенденций будущего развития институтов в рамках сотрудничества.

В результате проведенного качественного контент-анализа была составлена кодировальная матрица[[161]](#footnote-162), благодаря которой удалось выявить общие черты и различия в ожиданиях и дальнейших действиях ЕС и НАТО по вопросам будущего развития сотрудничества в этой сфере. В частности, совпадают следующие направления деятельности в области политики кибербезопасности: наибольшее количество совпадений в рамках повышения возможностей киберзащиты государств-членов и углубления сотрудничества с партнерами и заинтересованными сторонами; далее идет обеспечение высоких стандартов кибербезопасности для всех объектов инфраструктуры; а также привлечение специализированного персонала, инвестирование в обучение и инновации, повышение киберосведомленности посредством обмена опыта и информацией и подтверждение лидерства в реализации политики кибербезопасности.

На основе полученных данных представляется возможным определить модели потенциальных и альтернативных вариантов дальнейшего развития событий с помощью метода построения прогнозных сценариев[[162]](#footnote-163). Благодаря анализу факторов, связанных с прошлыми тенденциями развития и взаимодействия ЕС и НАТО, современной ситуацией, а также индивидуальными и коллективными ожиданиями и направлениями деятельности организаций, отраженными в стратегических документах, были определены полярные тенденции, связанные с будущим развитием сотрудничества организаций и факторы, которые влияют на развитие тех или иных трендов[[163]](#footnote-164). Для построения сценариев взято ограничение по времени до 2030 года, так как именно этими рамками ограничивается большинство стратегических документов рассматриваемых структур, однако в прогнозную таблицу включены и глобальные факторы, вероятность которых может быть подтверждена намного позже или не подтверждена совсем.

**Первый сценарий** – расширение сотрудничества ЕС и НАТО. Его можно учитывать как базовый, если брать во внимание актуальный на 2022 г. вектор развития отношений организаций. Этому сценарию соответствует направление деятельности акторов, отраженное в стратегических документах и связанное с необходимостью углубления сотрудничества с партнерами и заинтересованными сторонами.

Интеграция европейской общей политики безопасности и обороны приведет к дальнейшему расширению возможностей ЕС в военном секторе, что потребует переформатирования сотрудничества ЕС и НАТО для повышения эффективности их совместной деятельности. Данная тенденция сможет наблюдаться при снижении межгосударственных противоречий между странами, сокращении влияния США на политику европейских стран, а также повышении влияния транснациональных корпораций на оборонно-промышленный комплекс и политику ЕС.

Политическая и оборонная консолидация государств трансатлантического пространства будет способствовать увеличению взаимного доверия для расширения взаимодействия ЕС и НАТО в области реализации политики кибербезопасности. Она может быть опосредована разработкой общих подходов для сотрудничества, определением общих концепций, преодолением разногласий между государствами трансатлантического пространства и осознанием необходимости объединения усилий перед лицом совместных угроз, вызванных действиями внешних акторов (например, РФ или КНР), а также политической нестабильностью в соседних регионах.

Дальнейшая институционализация сотрудничества ЕС и НАТО будет способствовать расширению их двусторонних отношений. В рамках реализации данного сценария может потребоваться ряд консолидированных действий, которые были определены исследователями трансатлантического сотрудничества ЕС и НАТО Б. Лете и П. Перником[[164]](#footnote-165).

Во-первых, исследователи предлагают создать единый информационный центр ЕС-НАТО по киберугрозам. Миссия такого центра заключалась бы в улучшении обмена информацией путем налаживания отношений между организациями и их государствами-членами. Например, сегодня еще остается актуальной проблема раскрытия секретной информации, особенно в отношениях таких государств как Турция, Кипр и Греция. Подобный центр помог бы решить данные противоречия путем консультирования по стандартным операционным процедурам технического и оперативного уровня для обмена информацией между подразделениями ЕС и НАТО, и определения того, как обеспечить безопасные линии связи для обмена конфиденциальными разведданными. Центр мог бы определить эффективными платформы для обмена или облачные пространства для хранения информации, которые могут противостоять все более сложным атакам на основе открытых отраслевых спецификаций. Тем более, что пункт о повышении осведомленности включен в стратегические документы обеих организаций. Подобная платформа позволила бы внести конкретные предложения о том, как использовать постоянное структурированное сотрудничество по вопросам обороны и безопасности ЕС (PESCO) и Европейский фонд обороны (EDF). Более того, предложение государств-членов ЕС о разработке «Платформы обмена информацией о киберугрозах и реагировании на инциденты» в рамках PESCO[[165]](#footnote-166) подталкивает на мысль о том, что данную инициативу члены Союза могли бы расширить для НАТО в рамках устранения возникшего пробела в обмене информацией.

Во-вторых, представляется возможным создание Целевой группы ЕС-НАТО для координации процессов реагирования на киберкризисы. Существующие структуры, которые позволяют организациям консолидировать свои усилия по-прежнему ограничены, начиная от официальных и неформальных встреч между Североатлантическим советом и Комитетом ЕС по политике и безопасности и заканчивая обменом мнениями на министерских встречах и перекрестных брифингах для соответствующих учреждений. Именно поэтому встает необходимость создания дорожной карты для коллективных действий. Однако, создание такой Целевой группы потенциально станет возможным только когда крупный инцидент станет угрозой для государств-членов ЕС и НАТО, и самих организаций. В истории уже были подобные случаи, например, описанные раннее WannaCry и NonPetya, однако это не стало стимулом к подобным действиям, так как в ЕС и НАТО все еще отсутствует единое понимание концептов киберкризиса и киберугрозы. В связи с этим, первоначальное значение имеет определение скоординированного подхода с прицелом на создание единой Целевой группы.

В-третьих, необходимо разработать механизмы для коллективного реагирования на кибератаки. Сегодня ЕС и НАТО уже проводят совместные киберучения и обмениваются образовательными практиками, чтобы создать единые политические и оборонные инструменты для проведения наступательной стратегии и применения определенных санкций к нарушителям норм и правил безопасного киберпространства. НАТО уже признает кибератаку на одного из союзников как повод применения Статьи 5 Североатлантического договора. ЕС, со своей стороны, создал в 2017 году свой инструментарий кибердипломатии, как основу для дипломатического ответа на вредоносную атаку. Все эти меры повысили индивидуальные возможности организаций, но в настоящий момент нет подобных инструментов, равно как и соглашений об условиях, которые привели бы к коллективному использованию этих механизмов.

В-четвертых, для выполнения вышеуказанных рекомендаций следует создать общий Целевой фонд в области кибербезопасности для стран-партнеров. Такая структура позволила бы восполнить важный пробел, сосредоточив внимание на развитии местных и низовых навыков в области кибербезопасности и дать возможность различным заинтересованным сторонам в странах-партнерах посещать киберкурсы, семинары, тренинги и конференции ЕС или НАТО, или организовывать аналогичные виды деятельности у себя в стране. В прошлом организации совместно работали над программами финансовой помощи, такими как регулярные взносы ЕС в целевые фонды НАТО для утилизации неразорвавшихся боеприпасов и инициативы по борьбе с коррупцией, поэтому создание подобного независимого фонда могло бы оказаться вполне реально выполнимой задачей.

Наконец, возвращаясь к общему направлению по расширению сотрудничества с партнерами и заинтересованными сторонами, можно дать рекомендацию, согласно которой ЕС и НАТО могли бы стать лидерами в формировании глобальных норм поведения государств в киберпространстве. Отсутствие международного соглашения о правилах, регулирующих поведение государств в киберпространстве, или о механизмах «цифровой самообороны» усложняет усилия по управлению трансграничными киберугрозами. Таким образом, ЕС и НАТО, как две организации с общими целями и пересекающимися членскими составами, имеют возможность сформировать свое собственное общее видение ответственного поведения национальных государств в киберпространстве и спроецировать его на мировую арену. В этом контексте организации должны наладить диалог том, как они могут помочь работе, проводимой Группой правительственных экспертов ООН по информационной безопасности (UNGGE) – платформой ООН, предназначенной для обсуждения применимости международного права в киберпространстве. Сотрудничество ЕС-НАТО также может быть использовано для продвижения идей о прозрачности и подотчетности в киберпространстве на других международных платформах, от G20 до ОЭСР или ОБСЕ[[166]](#footnote-167).

Препятствием для реализации данного сценария могут стать тенденции, связанные с деградацией общей политики безопасности и обороны ЕС, поскольку в таком случае сотрудничество с НАТО будет иметь характер не взаимодополняемости, а зависимости, с чем могут не согласиться многие страны-члены ЕС. Кроме того, такие факторы как определение стратегической автономии ЕС от НАТО, установление более тесных отношений между европейскими странами и РФ или КНР, межгосударственные противоречия, продолжение дублирования функций организациями могут помешать развитию данного сценария.

**Второй сценарий** – статус-кво в рамках взаимодействия ЕС и НАТО в киберсфере. Дальнейшая интеграция ЕС в области обороны и безопасности не приведет его к укреплению взаимодействия с НАТО при наличии разногласий между странами трансатлантического пространства безопасности. Такие разногласия могут быть связаны с усилением роли третьих стран в регионе, конфликтами в соседних странах или, наоборот, замораживанием и разрешением этих конфликтов, в связи с чем дальнейшее расширение сотрудничества будет просто бессмысленным.

Организации поймут, что рационально будет остаться на том же уровне отношений, который на сегодняшний день уже приносит преференции обеим структурам. С одной стороны, ЕС получает опыт в рамках расширения оборонных возможностей в области противостояния киберугрозам, с другой стороны, НАТО имеет возможность контролировать политические процессы в европейских странах, а также их намерения в отношении других акторов международных отношений. Дальнейшая институционализация сотрудничества ЕС и НАТО в кибербезопасности будет ограничена возрастающим влиянием государств-членов на процесс принятия решений в рамках организаций и их нежеланием расширять возможности обмена информацией и разведданными.

При этом возникновение новых общих для обеих организаций угроз, решение всех межгосударственных противоречий, развитие ЕС и НАТО в сфере оборонных возможностей скорей всего потребуют от организаций определенных действий для развития сотрудничества и создания новых инструментов и механизмов, которые не позволят остаться отношениям ЕС и НАТО на прежнем уровне.

**Третий сценарий** – деградация сотрудничества ЕС и НАТО в сфере обеспечения кибербезопасности. Это подразумевает не распад институтов, что маловероятно, а неэффективность их совместной деятельности, осознание того, что дальнейшее сотрудничество не рационально для обеих структур и далее следует опираться только на собственные силы и международные форматы за рамками ЕС и НАТО. Этому сценарию способствуют тенденции усиления разногласий между государствами трансатлантического пространства безопасности и сохранения статуса-кво в институтах ЕС и НАТО. Кроме того, этот сценарий возможен как при укреплении интеграции ЕС в области обороны и безопасности, так и при ее деградации. В первом случае проект стратегической автономии продолжит развиваться и приведет к созданию в ЕС полного спектра оборонного потенциала, в том числе, и в сфере обеспечения надежной кибербезопасности. Во втором – новые инициативы ЕС не достигнут поставленных целей, а межнациональные противоречия не позволят общей внешней политике стать наднациональным вопросом в повестке организации.

В отношениях ЕС с НАТО может выйти на первый план проблема дублирования некоторых функций или разногласий в рамках создания скоординированного подхода к политике кибербезопасности. Выше уже были перечислены те проблемы, с которыми сталкиваются структуры в построении сотрудничества в области кибербезопасности, среди которых неравные возможности государств-членов, отсутствие единых каналов обмена информацией и разведданными и нежелание национальных правительств передавать их на наднациональный уровень. Все эти препятствия могут помешать созданию совместных норм и правил, а также углублению сотрудничества для защиты критической инфраструктуры и иных процессов в киберпространстве. Однако, реализации третьего сценария может препятствовать выполнение тех упомянутых выше условий, при которых сотрудничество ЕС и НАТО будет только расширяться и углубляться.

Более того, существуют и глобальные факторы, от которых напрямую не зависит развитие отношений ЕС и НАТО в рамках трансатлантического пространства безопасности. Однако, будучи одним из элементов системы международных отношений, трансатлантическое политическое пространство все же может оказаться под влиянием этих факторов, которые косвенно сыграют роль в отношениях ЕС и НАТО или во взаимодействии государств-членов организаций.

**Выводы к главе.** Сотрудничество ЕС и НАТО необходимо для содействия эффективному и многостороннему реагированию на современные угрозы безопасности. Приоритетным направлением в рамках этого взаимодействия является сфера кибербезопасности, в области которой организации уже добились значительных успехов и продолжают развивать коллективные меры для реагирования на киберугрозы. Основными достижениями в сотрудничестве ЕС и НАТО в сфере кибербезопасности являются заключение Технического соглашения по киберзащите между Техническим центром НАТО по реагированию на компьютерные инциденты (NCIRC) и Группой реагирования на компьютерные чрезвычайные ситуации ЕС (CERT-EU); проведение ежегодных совместных киберучений; обмен опытом и передовыми практиками. Однако, углублению и расширению сотрудничества между организациями в киберсфере препятствуют проблемы, с которыми сталкиваются ЕС и НАТО в данном процессе, связанные с неравными возможностями государств-членов, отсутствием единых каналов обмена информацией и разведданными и нежеланием национальных правительств передавать их на наднациональный уровень. В связи с этим представляется возможным прогнозирование трех сценариев дальнейшего развития отношений организаций: 1) расширение и углубление взаимодействия; 2) статус-кво в отношениях; 3) деградация и неэффективность совместной деятельности.

В целом, сложно учесть все факторы и процессы, которые могут повлиять на сотрудничество ЕС и НАТО в сфере кибербезопасности. До тех пор, пока не сформируется относительно стабильный мировой порядок, который будет основан на легитимных и авторитетных международных институтах, система международных отношений будет продолжать динамично меняться, будут появляться новые и трансформироваться старые вызовы безопасности, обе организации будут определять приоритеты своей деятельности и новых партнеров для выстраивания сотрудничества в областях, соответствующих интересам сторон и считающихся рациональными с точки зрения установления внешних связей. Однако можно сказать определенно, что новый этап развития взаимодействия ЕС и НАТО в сфере кибербезопасности приведет к новым моделям сотрудничества или, наоборот, противостояния между организациями.

# **ЗАКЛЮЧЕНИЕ**

Глобальное использование информационно-коммуникационных технологий поставило на повестку дня актуальный вопрос обеспечения информационной безопасности или кибербезопасности, которая, имея транснациональный характер, не может рассматриваться только на уровне отдельных государств, а требует единого ответа от наднациональных структур и иных международных институтов. Примером подобного взаимодействия выступает сотрудничество ЕС и НАТО по вопросам кибербезопасности, которое стало предметом настоящего исследования. В рамках работы была поставлена цель определить перспективы развития сотрудничества организаций в данной киберсфере на основе анализа подходов ЕС и НАТО к политике кибербезопасности. Цель исследования была реализована посредством выполнения ряда задач.

*Первая задача* заключалась в операционализации понятия кибербезопасность. На основе теории секьюритизации были проанализированы основные подходы к пониманию терминов киберпространства, киберугроз и кибербезопасности, а также референтные объекты информационной безопасности и направления оптимизации деятельности по защите киберпространства. В итоге в настоящем исследовании «кибербезопасность» стала определяться как совокупность технологий, процессов, практик и мер реагирования, предназначенных для защиты информационно-коммуникационных систем, в том числе компьютеров, программ и данных, от повреждения, несанкционированного использования и модификации с целью обеспечения их конфиденциальности и целостности.

*Вторая задача* была посвящена исследованию подходов к анализу сотрудничества ЕС и НАТО в сфере кибербезопасности. Научные и аналитические работы зарубежных и отечественных исследователей позволили сделать вывод о том, что на сегодняшний день ЕС и НАТО наращивают собственный потенциал и продолжают сотрудничество в области безопасности и обороны, в частности, в сфере защиты критической инфраструктуры от кибератак. Однако, изучению взаимодействия организаций по вопросам кибербезопасности посвящено не так много научных работ, поэтому в рамках настоящего исследования был проведен комплексный анализ аспектов сотрудничества двух организаций, подходов акторов к политике кибербезопасности, а также выявлены проблемы и перспективы расширения отношений в данной сфере.

Проанализировать и сравнить подходы ЕС и НАТО к политике кибербезопасности позволила реализация *третьей и четвертой задач* исследования. Благодаря сравнительному анализу были определены общие черты и особенности организаций в рамках реализации политики кибербезопасности. Схожими характеристиками оказались наличие постоянно действующей нормативно-правовой базы и широкий ряд специальных институтов и инструментов, цели организаций, похожие действия, которые предпринимаются для защиты критической инфраструктуры, а также определение перспектив развития. Основные отличия были отмечены в превосходстве НАТО в проведении киберучений и предоставлении образовательных практик, а также преимуществах ЕС в наличии специальных фондов финансирования перспективных проектов в киберсфере.

*Пятая задача* позволила вывить институционально-правовые аспекты и основные проблемы взаимодействия ЕС и НАТО в сфере кибербезопасности на современном этапе. В частности, был сделан вывод о том, что организации уже достигли значительных успехов в выстраивании сотрудничества в кибернетической сфере, однако его расширению и углублению препятствует ряд факторов, среди которых неравные возможности государств-членов, отсутствие единых каналов обмена информацией и разведданными и нежелание национальных правительств передавать их на наднациональный уровень.

В связи с этим в рамках реализации *шестой задачи* были определены возможные перспективы развития сотрудничества ЕС и НАТО в сфере кибербезопасности. Качественный контент-анализ позволил определить основные направления деятельности организаций, которые они выделяют в качестве приоритетных для будущего развития собственного потенциала и коллективных возможностей. Эти направления в совокупности с анализом прошлых и современных тенденций сотрудничества ЕС и НАТО в сфере кибербезопасности, позволили спрогнозировать возможные перспективы развития взаимодействия структур, которые были сведены к трем основным сценариям, первый из которых стал базовым, а два других – альтернативными.

В ходе исследования автор пришел к выводу о том, что обе научные гипотезы, которые были определены в начале исследования, могут быть подтверждены в рамках анализа будущего развития отношений ЕС и НАТО в области обеспечения политики кибербезопасности. С одной стороны, возможно дальнейшее расширение и углубление сотрудничества с учетом наличия общих ценностей и способов реализации защиты критической инфраструктуры, а также обеспечения стабильности в киберпространстве в рамках подходов организаций к политике кибербезопасности. При этом каждый из акторов продолжит преследовать свои цели и продвигать собственные интересы. С другой стороны, дальнейшее построение общей политики кибербезопасности может остановиться на данном этапе или начать регрессировать по причине принципиальных различий в подходах ЕС и НАТО, а также из-за продолжающегося дублирования функций.

Таким образом, развитие сотрудничества будет зависеть от тех тенденций, согласно которым будут развиваться отношения ЕС и НАТО в будущем, а также факторов, в том числе и глобальных, которые окажут влияние на эти процессы. В целом, ускоряющиеся изменения в эпоху цифровых технологий и связанные с ними проблемы заставляют традиционные структуры межправительственных организаций, таких как ЕС или НАТО, идти по пути развития и создания новых инструментов и механизмов для противодействия возникающим вызовам. Это также подчеркивает, как этим традиционным структурам может быть трудно координировать свои действия друг с другом, даже если для этого есть взаимные интересы. Однако и ЕС, и НАТО будут продолжать сталкиваться с угрозами, исходящими от киберпространства, поэтому медленно, но верно разрабатываются общие ответные меры для укрепления авторитета организаций в киберпространстве в глазах их членов, партнеров и оппонентов. Очевидно, что ЕС и НАТО должны перейти от повестки дня, которая укрепляет их механизмы координации, обмена и консультаций, к инициативам, которые улучшают их совместные функции по наращиванию сил, кибернетические возможности, структуры связи и механизмы принятия решений в киберучениях, кризисах и конфликтах, а также их взаимодействие с партнерами в киберпространстве. Развитие сотрудничества ЕС и НАТО в киберпространстве уже происходит из-за возникновения новых общих угроз и усиления роли других международных институтов и государств, но потребуется еще больше усилий, чтобы адаптироваться к цифровой эпохе, которая постоянно и быстро развивается.

# **СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

*Источники*

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ // Консультант Плюс. URL: <http://www.consultant.ru/document/cons_doc_LAW_61798/> (дата обращения: 10.02.2022).

A Digital Agenda for Europe // European Commission. – Brussels, 19.5.2010, COM (2010)245. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> (дата обращения: 20.03.2022).

A Europe fit for the digital age // The European Commission’s priorities. – European Commission, 2019. URL: <https://ec.europa.eu/info/strategy/priorities-2019-2024_en> (дата обращения: 20.03.2022).

Brussels Summit Communiqué // NATO. – Press Release (2021) 086. 14.6.2021. URL: <https://www.nato.int/cps/en/natohq/news_185000.htm> (дата обращения 15.03.2022).

CCDEOE official page. URL: <https://ccdcoe.org/history.html> (дата обращения: 15.03.2022).

Combatting Fraud and Counterfeiting of Non-Cash Means of Payment // European Commission. URL: <https://ec.europa.eu/home-affairs/pages/page/combatting-fraud-and-counterfeiting-non-cash-means-payment_en> EN (дата обращения: 20.03.2022).

Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization // NATO. – Press Release (2017) 174. 5.12.2017. URL: <https://www.nato.int/cps/en/natohq/official_texts_149522.htm> (дата обращения: 11.05.2022).

Cyber Defence // NATO. 23.3.2022. URL: <http://www.nato.int/cps/en/natohq/topics_78170.htm> (дата обращения 15.03.2022).

Cyber Defence Pledge // NATO. – Press Release (2016) 124, 8.7.2016. URL: <https://www.nato.int/cps/en/natohq/official_texts_133177.htm> (дата обращения 15.03.2022).

Cyber Threats and Incident Response Information Sharing Platform (CTIRISP) // PESCO Projects. URL: <https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/> (дата обращения: 13.05.2022).

Cybersecurity Policies // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq8796b> (дата обращения: 20.03.2022).

Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace // European Commission. – Brussels, 7.2.2013, JOIN (2013) 1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN> (дата обращения: 20.03.2022).

CyCLONe official page. URL: <https://www.cyclone-project.eu/> (дата обращения: 20.03.2022).

Defending the networks: the NATO Policy on Cyber Defence // NATO. 19.8.2011. URL: <https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf> (дата обращения 15.03.2022).

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, July 6 2016 // Official Journal of the European Union. – 19.7.2016, L 194/1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1> (дата обращения: 20.03.2022).

Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing of 13 December 2011 // Official Journal of the European Union. – 17.12.2011, L 335/1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093> (дата обращения: 20.03.2022).

Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision of 12 August 2013 // Official Journal of the European Union. – 14.8.2013, L 218/8. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040> (дата обращения: 20.03.2022).

Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”) // Council of the European Union. – Brussels, 7.6.2017, 9916/17. URL: <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (дата обращения: 20.03.2022).

EC3 official page. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения 20.03.2022).

ENISA Mandate and Regulatory Framework // ENISA. URL: <https://www.enisa.europa.eu/about-enisa/regulatory-framework> (дата обращения: 20.03.2022).

ENISA official page. URL: <https://www.enisa.europa.eu/about-enisa> (дата обращения 05.05.2022); CSIRTs Network // ENISA. URL: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network?tab=details> (дата обращения: 05.05.2022);

EU cybersecurity initiatives: working towards a more secure online environment, Factsheet // European Commission. 01.2017. URL: <https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf> (дата обращения: 20.03.2022).

Europe 2020: a strategy for smart, sustainable and inclusive growth // European Commission. – Brussels, 3.3.2010, COM (2010) 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC2020&from=en (дата обращения: 20.03.2022).

Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 16.06.2020. URL: <https://www.consilium.europa.eu/media/44451/200616-progress-report-nr5-eu-nato-eng.pdf> (дата обращения: 11.05.2022).

Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017 // NATO. 17.06.2019. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf> (дата обращения: 11.05.2022).

Geneva Dialogue for Responsible Behaviour in Cyberspace in the context of international peace and security // Baseline study. 6. 2019. – P. 6–9. URL: <https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Baseline-Study.pdf> (дата обращения: 13.05.2022).

German National Cyber Security Strategy // Federal Ministry of the Interior. 09.09.2021. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany (дата обращения: 10.02.2022).

A Global Strategy for the European Union’s Foreign and Security Policy. Shared Vision, Common Action: A Stronger Europe // Council of the European Union. – Brussels, 14.11.2016. URL: https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy\_en (дата обращения: 20.03.2022).

Hybrid threats as a concept // Hybrid CoE. URL: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> (дата обращения: 20.02.2022).

Joint Cybercrime Action Taskforce (J-CAT) // Europol. URL: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce> (дата обращения: 05.05.2022).

Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO // NATO. – Press Release (2016) 119. 8.07.2016. URL: <https://www.nato.int/cps/en/natohq/official_texts_133163.htm> (дата обращения: 11.05.2022).

Joint declaration on EU-NATO cooperation by President of the European Council, President of the European Commission, and Secretary General of NATO // European Council. Council of the European Union. – Press Release. 10.07.2018. URL: <https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf> (дата обращения: 11.05.2022).

Law enforcement agencies across the EU prepare for major cross-border cyber-attacks // Europol. – News, 18.03.2019. URL: <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks> (дата обращения: 20.03.2022).

Lisbon Summit Declaration issued by the Heads of state and Government participating in the meeting of the North Atlantic Council in Lisbon // NATO. – Press Release (2010) 155, 20.11.2010. URL: <https://www.nato.int/cps/em/natohq/official_texts_68828.htm> (дата обращения 15.03.2022).

List of data breaches in 2021 // IT Governance. URL: <file:///C:/Users/%D0%B0%D1%81%D1%83%D1%81/Downloads/2021_data_breach_infographic.pdf> (дата обращения: 10.02.2022).

Memorandum of understanding // NATO, 3.11.2008. URL: <https://www.nato.int/cps/en/natohq/official_texts_18839.htm?selectedLocale=en> (дата обращения: 15.03.2022).

NATO 2030: United for a New Era // NATO Defense College. 25.11.2020. – P. 45. URL: <file:///C:/Users/%D0%B0%D1%81%D1%83%D1%81/Downloads/201201reflectiongroupfinalreportuni_01AA68FEB78CE059F77DA9F2DD4BFC98_75365_wfOiUrW14oBjHRPNn7tVylgBaI_76960.pdf> (дата обращения: 15.03.2022).

NATO Allies and partners participate in large-scale cyber defence exercise // NATO. – News. 29.4.2022. URL: <https://www.nato.int/cps/en/natohq/news_194902.htm?selectedLocale=en> (дата обращения: 15.03.2022).

NATO and the European Union enhance cyber defence cooperation // NATO. – News. 10.02.2016.URL: <https://www.nato.int/cps/en/natohq/news_127836.htm?selectedLocale=en> (дата обращения: 11.05.2022).

NATO Cyber Defence, Factsheet // NATO, 2.2019. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf> (дата обращения: 15.03.2022).

NATO Cyber Defence, Factsheet // NATO, 4.2017. URL: https://www.nato.int/nato\_static\_fl2014/assets/pdf/pdf\_ 2018\_02/20180213\_1802-factsheet-cyber-defence-en.pdf (дата обращения: 15.03.2022).

NATO presents the Agenda for 2030 // European Commission. – News. 9.6.2021. URL: <https://ec.europa.eu/newsroom/cipr/items/713800/en> (дата обращения: 15.03.2022).

NATO's Cyber Security Centre // NATO Communications and Information Agency. URL: <https://www.ncia.nato.int/what-we-do/cyber-security.html> (дата обращения: 15.03.2022).

NCI Agency official page. URL: <https://www.ncia.nato.int/> (дата обращения: 05.05.2022); Cyber Defence // NATO. URL: <https://www.nato.int/cps/en/natohq/topics_78170.htm> (дата обращения: 05.05.2022); CCD CE official page. URL: <https://ccdcoe.org/> (дата обращения: 05.05.2022).

NSO official page. URL: <https://www.natoschool.nato.int/> (дата обращения: 05.05.2022).

On Critical Information Infrastructure Protection “Achievements and next steps: towards global cyber-security” // European Commission. – Brussels, 31.3.2011, COM (2011) 163. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF> (дата обращения: 20.03.2022).

Permanent Structured Cooperation (PESCO) official page. URL: <https://www.pesco.europa.eu/> (дата обращения: 20.03.2022).

PESCO: EU paves way to defense union // Deutsche Welle. 13.11.2017. URL: <https://www.dw.com/en/pesco-eu-paves-way-to-defense-union/a-41360236> (дата обращения 20.03.2022).

Prague Summit Declaration // NATO. – Press Release (2002) 127. 21.11.2002. URL: <https://www.nato.int/cps/en/natohq/official_texts_19552.htm> (дата обращения: 15.03.2022).

Proposal for directive on measures for high common level of cybersecurity across the Union // European Commission. – 16.12.2020. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union> (дата обращения: 20.03.2022).

1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // Official Journal of the European Union. – 7.6.2019, L 151/15. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC> (дата обращения: 20.03.2022).

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU // European Commission and High Representative of the Union for Foreign Affairs and Security Policy. – Brussels, 13.9.2017, JOIN (2017) 450. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en (дата обращения 20.03.2022).

Sharing malware information to defeat cyber attacks // NATO, 29.11.2013. URL: <https://www.nato.int/cps/en/natolive/news_105485.htm> (дата обращения: 15.03.2022).

Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 3.06.2021. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf> (дата обращения: 11.05.2022).

Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon // NATO. 19.11.2010. URL: <https://www.nato.int/cps/en/natohq/official_texts_68580.htm> (дата обращения: 15.03.2022).

Strengthening Europe Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry // European Commission. – Brussels, 5.7.2016, COM (2016) 410. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=EN (дата обращения: 20.03.2022).

Swedish National Cyber Security Strategy // Government offices of Sweden. 22.06.2017. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy (дата обращения: 10.02.2022).

The Cybersecurity Strategy // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy> (дата обращения 20.03.2022).

The European Agenda on Security // European Commission. – Brussels, 28.4.2015, COM (2015) 185. URL: https://ec.europa.eu/home-affairs/system/files/2020-09/eu\_agenda\_on\_security\_en\_0.pdf (дата обращения: 20.03.2022).

The European Cybersecurity Certification Group // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group> (дата обращения: 20.03.2022).

Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 8.06.2018. – P. 4. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf> (дата обращения: 11.05.2022).

*Литература*

1. Атаманов Г.А. Информационная безопасность: сущность и содержание / Г.А. Атаманов // Бизнес и безопасность в России. – 2007. №47. – С. 104–109.

Ахременко А.С. Политический анализ и прогнозирование: введение в количественные методы. Учебное пособие / А.С. Ахременко. – М.: Из-во МГУ, 2012. – 345 с.

1. Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. №1 (2) – С. 22–27.

Богатуров А.Д. Очерки теории и методологии политического анализа международных отношений / А.Д. Богатуров, Н.А. Косолапов, М.А, Хрусталев. – М.: НОФМО, 2002. – 390 с.

Богданов А.А. Тектология: всеобщая организационная наука / А.А. Богданов. – М., 1989. – URL: <https://gtmarket.ru/library/basis/5909> (дата обращения: 15.02.2022).

Буденный А.А. НАТО и военно-политическая независимость Западной Европы / А.А. Буденный // США и Канада: экономика, политика, культура. – 2018. № 4. – С. 98–105.

1. Бухарин С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов – М.: Академический проект, 2007. – 382 с.
2. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев – М.: Харвест, 2004. – 426 с.
3. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты перспективы: дис. д. полит. наук: 23.00.04. – МГИМО МИД, Москва, 2017. – 332 с.

Казаковцев А.В. НАТО и кибербезопасность / А.В. Казаковцев // Вестник Волгоградского гос. ун-та. – 2012. № 2(22). – С. 109–114.

1. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. – 2017. № 6 – С. 44–51.
2. Кардава Н.В. Политика обеспечения кибербезопасности в Европейском Союзе: национальный и наднациональный уровни / Н.В. Кардава // Каспийский регион: политика, экономика, культура – 2019. № 3(60). – С. 73–78.
3. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. наук: 12.00.03. – Москва, 2016 – 66 с.

Козубенко И.И. Институциональное взаимодействие структур ЕС и НАТО / И.И. Козубенко // Новое слово в науке: перспективы развития. – 2016. № 2 (8). – С. 39–42.

Косолапов Н.А. Транснациональные политические пространства: явление и практика / Н.А., Косолапов, М.В. Стрежнева, И.Л. Прохоренко, Ф.Г. Войтоловский. – М: Весь мир, 2011. – 234 с.

Курылев К.Л. Цифровая зависимость НАТО / К.Л. Курылев, В.Т. Цаканян // Вестник Моск. гос. областного ун-та. Серия: История и политические науки. – 2018. №1. – С. 45–53.

1. Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин. – СПб: Фонд Университет, 2000. – 288 с.
2. Макаров В.Е. Политические и социальные аспекты информационной безопасности: монография – Таганрог: Изд. С.А. Ступин, 2015. – 351 с.

Манойло А.В. Современные стратегии кибербезопасности и киберобороны НАТО / А.В. Манойло // Актуальные проблемы Европы. – 2020. №3. – С. 160–184.

Пантин В.И. Кибербезопаность: проблемы формирования единой политики в Европейском Союзе / В.И. Пантин, Н.В. Кардава, // Вестник Пермского университета. Политология. – 2018. №3. – С. 5–18.

1. Паршин С. А. Кибервойны – реальная угроза национальной безопасности / С. А. Паршин, Ю. Е. Горбачев, Ю. А. Кожанов – М.: КРАСАНД, 2011. – 96 с.

Прохоренко И.Л. Пространственный подход в исследовании международных отношений / И.Л. Прохоренко. – М.: ИМЭМО РАН, 2015. – 111 с.

1. Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации: автореф. дис. канд. технич. Наук: 05.13.19. – СПбГУ ИТМО, Санкт-Петербург, 2008. – 145 с.

Стратегическая автономия ЕС и перспективы сотрудничества с Россией / под ред. Н.К. Арбатовой, А.М. Кокеева – М.: Весь мир, 2020. – 368 с.

1. Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» / А.А. Стрельцов // Информационное общество. – 2001. №. 4. – 52 с.

Тузовская Н.Ю. Пределы «Стратегического партнерства» ЕС и НАТО / Н.Ю. Тузовская // Актуальные проблемы Европы. – 2010. – С. 93–94.

1. Чеботарева А.А. Научные подходы к определению понятия «информационная безопасность» / А.А. Чеботарева // Информационное право. – 2011. №1. – С. 3–11.

Шариков П. Подходы США, ЕС и России к проблеме информационной политики / П. Шариков, Н. Степанова // Современная Европа. – 2019.№2. – С. 73-83.

Шариков П.А. Военные аспекты кибербезопасности в контексте специальной военной операции РФ на территории Украины / П.А. Шариков // Аналитические записки Института Европы РАН. Выпуск II. – 2022, № 13(280). – С. 5–12.

Щербак И. Стратегическая автономия ЕС и проблемы формирования внешнеполитической повестки в эпоху пандемии / И. Щербак // Современная Европа. – 2020. №6. – С. 29–40.

Angelov I. The Security Environment and the Challenges to the European Union and NATO in the field of Security / I. Angelov // Security & Future. – 2019. № 3(1). – P. 17–21.

Berelson B. Content-analysis in communication research / B. Berelson. – Glencoe: Free Press, 1952. – 220 p.

Biscop S. EU-U.S. Consensus and NATO-EU Cooperation / eds. by T. Valasek. – Brussels: Carnegie Endowment for International Peace, 2019. URL: <https://carnegieendowment.org/files/NATO_int_final1.pdf>.

Buzan B. Security: A New Framework for Analysis. Boulder / B. Buzan, O. Wæver, J. De Wilde. – CO: Lynne Rienner Publishers, 1998. – 239 p.

Calderoni F. The European legal framework on cybercrime: striving for an effective implementation / F. Calderoni // Crime Law Soc Change. – 2010. №54. – P. 339–357.

1. Carr M. Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance // M. Carr, F. Lesniewska. – 2020. № 34(3). – P. 391–412.

Christou G. The challenges of cybercrime governance in the European Union / G. Christou // European Politics and Society. – 2018. – P. 1–21.

1. Clark D. Characterizing cyberspace: past, present and future / D. Clark // MIT CSAIL. 2010. URL: <https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf>.

Doctorow C. America’s broken digital copyright law is about to be challenged in court / C. Doctorow // The Guardian. 21.07.2016. URL: <https://www.theguardian.com/technology/2016/jul/21/digital-millennium-copyright-act-eff-supreme-court> (дата обращения: 10.02.2022).

Easton. D. The Political System. An Inquiry into the State of Political Science / D. Easton. – N.Y.: Knopf, 1953. – 177 p.

1. Fichtner L. What kind of cyber security? Theorizing cyber security and mapping approaches / L. Fichtner // Internet Policy Review. – 2019. №7 (2). – P. 1–19.

Fuster G.G. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights // G.G. Fuster, L. Jasmontaite // The Ethics of Cybersecurity. – 2020. – P. 97–115.

1. Gibson W. Neuromancer / W. Gibson. – Orion Publishing Group, 2016. – 314 p.

Goldgeier J. The Future of NATO. NATO Science for Peace and Security Series / J. Goldgeier // Human and Societal Dynamics. IOS Press. – 2011. №76. – P. 1–12.

1. Gomez M.A. Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats // M.A. Gomez, C. Whyte // Oxford Academic. – 2021. № 4(65). – P. 1137–1150.

Græger N. Grasping the everyday and extraordinary in EU–NATO relations: The added value of practice approaches / N. Græger // European Security. – 2017. № 26(3). – P. 340–358.

Guy P. B. Institutional Theory in Political Science / P.B. Guy. London: Pinter, 1999. – 205 p.

Hall P.A. Political Science and Three New Institutionalisms / P.A. Hall, R.C.R. Taylor // MPIFG Discussion Paper. – 1996. – 32 p.

1. Hansen L. Digital Disaster, Cyber Security, and the Copenhagen School / L. Hensen, H. Nissenbaum // International Studies Quarterly. – 2015. №53. – P. 1155–1175.

Healey J. NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow / J. Healey. K. T. Jordan // Atlantic Council. 9.2014. URL: <https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf> (дата обращения: 15.03.2022).

Helwig N. New Tasks for EU-NATO Cooperation An Inclusive EU Defence Policy Requires Close Collaboration with NATO / N. Helwig // German Institute for International and Security Affairs. – 2018. – P. 2–10.

Howorth J. EU–NATO cooperation: The key to Europe’s security future / J. Howorth // European Security. – 2017. № 26(3). – P. 454–459.

Howorth J. Strategic Autonomy and EU-NATO Cooperation: A Win-Win Approach / J. Howorth // L’Europe En Formation. – 2019. № 389(2). – P. 85–103.

Howorth J. The Euro-Atlantic Security Dilemma: France, Britain, and the ESDP / J. Howorth // Journal of Transatlantic Studies. – 2005. № 3(1). – P. 39–54.

Hughes R.B. NATO and Cyber Security: Mission accomplished? / R.B. Hughes // Charlise. – 2016. URL: http://www.carlisle.army.mil/ DIME/documents/ NATO%20 and%20 Cyber%20Defence.pdf.

1. Ilves L. K. European Union and NATO: Global Cybersecurity Challenges / L.K. Ilves, T.J. Evans, F.J. Cilluffo, A.A. Nadeau // PRISM. – 2016. № 2(6). – P. 126–141

Kaplan M.A. System and Process in International Politics / M.A. Kaplan. – Colchester: ECPR, 2005. – 260 p.

Kempf A. Considerations for NATO Strategy on Collective Cyber Defense / A. Kempf. – 2018. URL: http://csis.org/ blog /considerations-nato-strategy-collective-cyberdefens.

1. Kerschischnig G. Cyberthreats and International Law / G. Kerschischnig – The Hague, 2012. – 386 p.

Kovacs L. Cyber Security Policy and Strategy in the European Union and NATO / L. Kovacs // Land Forces Academy Review. – 2018. № 1(89). – P. 10–23.

Lete B. Cooperation in cyberspace / B. Lete // NATO Defense College. – 2019. – P. 33–43.

Lete, B. EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions / B. Lete, P. Pernik // German Marshall Fund of the United States. – 2017. URL: <https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions> (дата обращения: 15.02.2022).

1. Lezzi M. Cybersecurity for Industry 4.0 in the current literature: A reference framework / M. Lezzi, M. Lazoi, A. Corallo // Elsevier. Computers in Industry. – 2018. №103. – P. 97–123.

Light M. US and European perspectives on Russia / M. Light / eds. by J. Peterson, M. A. Pollack. Europe, America, Bush: Transatlantic relations in the twenty-first century. – London: Routledge. 2003. – 230 p.

McGee J. NATO and Cyber Defense: A Brief Overview and Recent Events / J. McGee. – 2011. URL: <https://www.csis.org/blog/natoand-cyber-defense-brief-overview-and-recentevents>.

1. Miron W. Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure / W. Miron, K. Muita // Technology Innovation Management Review. – 2014. – P. 33–39.
2. Mitchell G. E. Correlates of State-Sponsored Cyber Conflict / G.E. Mitchell, A. Pytlak // Routledge Handbook of International Cybersecurity / eds. by T. Eneken, M. Kerttunen. – Oxford, UK: Routledge, 2020. – 135 p.

Pernik P. Improving Cyber Security: NATO and the EU / P. Pernik // International Centre for Defence Studies. – 2014. – P. 17–25.

Poptchev P. NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages / P. Poptchev // Information and Security. – 2020. № 45. – P. 35–55.

Posen B. R. ESDP and the structure of world power / B.R. Posen // The International Spectator. – 2004. № 39(1). – P. 5–17.

1. Salminen M. The becoming of cyber-military capabilities / M. Salminen, M. Kerttunen // Routledge Handbook of International Cybersecurity / eds. by T. Eneken, M. Kerttunen. – Oxford, UK: Routledge, 2020. – P. 94–109.

Schmitt M. N. Tallinn Manual on the International Law Applicable to Cyber Warfare / M.N. Schmitt. – UK: Cambridge University Press, 2013. – 215 p.; Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M.N. Schmitt. – UK: Cambridge University Press, 2017. – 569 p.

Shopina I. Cybersecurity: legal and organizational support in leading countries, NATO and EU standards / I. Shopina, D. Khomiakov, N. Khrystynchenko, S. Zhukov, D. Shpenov // Journal of security and sustainability issues. – 2020. № 3(9). – P. 977–992.

Simion E. NATO-EU Cooperation / E. Simion // International Conference KNOWLEDGE-BASED ORGANIZATION. – 2018. № 24(1). – P. 211–214.

Simon J. S. The Father, the Son and the Holy Ghost: a Grounded Theory Approach to the Comparative Study of Decision-Making in the NAC and PSC // J. S. Simon, T. Nikola, G. Carmen // European Security. – 2017. № 3(26). – P. 359–379.

Smith M. E. Europe’s Foreign and Security Policy: The Institutionalisation of Cooperation / M.E. Smith. – Cambridge: Cambridge University Steven, 2004 – 209 p.

1. Stevens T. Global Cybersecurity: New Directions in Theory and Methods / T. Stevens // Politics and Governance. – 2018. № 6(2). – P. 1–11.
2. Walden I. Crime and Security in Cyberspace / I. Walden // Cambridge review of the International Affairs. – 2005. № 18(1). – P. 51–68.

Warleigh A. Influence and interest in the European Union: the new politics of persuasion and advocacy / A. Warleigh. – London: Europa Publications, 2002. – 265 p.

Wind M. Sovereignty and European Integration: Towards a Post Hobbesian Order / M. Wind. – Palgrave, 2001. – Pp. 40–42.

Zan T. EU-NATO Cyber Cooperation: Who Steps in During a Crisis? / T. Zan // Atlatic Voices. – 2017. № 9(7). – P. 5–11.

# **ПРИЛОЖЕНИЯ**

Приложение 1

Источник: составлено автором.

**Основные институты ЕС в сфере реализации политики кибербезопасности**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Название** | **Место** | **Функции** | **Формы деятельности** | **Члены** |
| Агентство по сетевой и информационной безопасности (ENISA) | Афины, Греция;  Ираклион,  Греция;  Брюссель,  Бельгия | - повышение надежности продуктов, услуг и процессов ИКТ;  - помощь Европе в подготовке к защите от киберугроз;  - обеспечение обмена знаниями и повышение осведомленности | - сотрудничество с государствами-членами и институтами ЕС;  - обучение персонала и структур ЕС, отвечающих за кибербезопасность;  - обучение IT-компаний, бизнес-структур и академического сообщества | страны-члены ЕС |
| Компьютерные группы реагирования на чрезвычайные ситуации (CSIRTs) | расположение в разных странах ЕС | - содействие развитию;  - укрепление доверия между странами-членами ЕС;  - создание условий для оперативного и близкого сотрудничества между государствами-членами | - предоставление площадки для сотрудничества, обмена информацией и укрепления доверия;  - помощь государствам-членам в скоординированном реагировании на киберугрозы | Швеция (22 команды);  Финляндия (5); Эстония (2);  Латвия (2);  Литва (8);  Дания (12);  Германия (49);  Нидерланды (29);  Бельгия (9);  Ирландия (3);  Франция (49);  Испания (75);  Португалия (42);  Чехия (56);  Польша (32);  Австрия (10);  Италия (32);  Словакия (13);  Венгрия (3);  Румыния (10);  Болгария (1);  Греция (6);  Кипр (2) |
| Европейская организация по кибербезопасности (ECSO) | Брюссель, Бельгия | - защита Европейского цифрового рынка от киберугроз;  - развитие рынка кибербезопасности в Европе;  - разработка и внедрение решения по кибербезопасности в отраслях, где Европа является лидером | - сотрудничество с ЕК и национальными правительствами для продвижения исследований и инноваций;  - разработка Стратегической программы НИОКР и Многолетней дорожной карты;  - продвижение и помощь в определении и реализации европейской промышленной политики в киберсфере;  - обучение в области ИКТ | Юридические лица, созданные в странах ЕС и Европейской ассоциации свободной торговли |
| Центр обмена и анализа информации (ISAC) | расположение в разных странах ЕС | - определение текущих проблем, с которыми сталкиваются частный и государственный сектора в киберсфере;  - предоставление информации об ISAC в Европе;  - предложение рекомендаций по работе ISAC в Европе;  - исследование роли ENISA в обеспечении киберзащиты | - сбор информации о киберугрозах;  - обеспечение двустороннего обмена информацией между частными и государственными секторами | бизнес-эксперты из разных стран-членов ЕС |
| Объединенный исследовательский центр (JRC) | Брюссель, Бельгия | - проведение исследований с целью предоставления независимых научных рекомендаций и поддержки политике ЕС | - разработка инновационных инструментов, доступных для всех политиков;  - передача знаний для поддержки европейской политики;  -проведение исследований, финансируемых Евратомом |  |
| Европейский центр по борьбе с киберпреступностью при Европоле (EC3) | Гаага, Нидерланды | - укрепление мер по реагированию правоохранительных органов на киберугрозы в ЕС;  - оперативная, стратегическая, аналитическая и судебная поддержка расследований государств-членов | - поддержка операций и расследований, проводимых государствами-членами;  - поддержка структурам кризисного управления ЕС;  - поддержка обучения и наращивания потенциала | страны-члены ЕС |

Источник: составлено автором на основе данных с официальных сайтов институтов ЕС[[167]](#footnote-168).

Приложение 2

Источник: составлено автором.

**Основные институты НАТО в сфере реализации политики кибербезопасности**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Название** | **Место** | **Функции** | **Формы деятельности** | **Члены** |
| Агентство связи и информации  (NCIA) | Брюссель, Бельгия;  Гаага, Нидерланды;  Монс, Бельгия | - предоставление передовых технологий командования, управления, связи, разведки и наблюдения в поддержку лиц, принимающих решения и осуществляющих кибермиссии;  - приобретения технологий, проектирование и разработка эффективных систем;  - централизованное планирование, проектирование систем, внедрение и управление их конфигурацией  - информационный обмен | - создание и поддержание консультационных и командных сетей НАТО;  - управление Академией связи и информации;  - анализ и оборонное планирование;  - сервисная поддержка и услуги бизнес-приложений;  - командование противовоздушной и противоракетной обороны;  - разведка, наблюдение, рекогносцировка;  - поддержка учений и операций;  - предоставление цифровых рабочих мест | 29 стран в Европе и Северной Америке |
| Технический центр по реагированию на компьютерные инциденты (NCIRC) | Монс, Бельгия | - содействие обнаружению, реагированию и предотвращению инцидентов в киберпространстве | - предоставление технических услуг в области кибербезопасности по всей территории НАТО  - обработка информацию об инцидентах и ее предоставление союзникам по НАТО | страны-члены НАТО |
| Центр передового опыта по совместной киберзащите  (CCD CE) | Эстония, Таллинн | - методологическое обеспечение киберопераций;  - подготовка кадров;  - налаживание взаимодействия между членами НАТО;  - информационный обмен с партнерами НАТО | - мониторинг информационных сетей;  - международные учения;  - международные конференции;  - издание пособий по кибероперациям | 28 государств-членов НАТО Финляндия  Швеция Япония Южная Корея  Швейцария  Ирландия |
| Центр киберопераций НАТО | Монс, Бельгия | - планирование военных операций  -интеграция кибернетических возможностей союзников;  - повышение осведомленности об обстановке в киберпространстве | - предоставление союзникам по НАТО необходимых инструментов и инфраструктуру для проведения операций в киберпространстве | страны-члены НАТО |
| Школа НАТО | Обераммергау, Германия | - коллективное и индивидуальное обучение с целью разработки будущей стратегии, политики, доктрин и процедур НАТО;  - создание глобально ориентированной системы обучения | - проведение межнациональных программ обучения, которые охватывают гражданский и военный персонал | страны-члены НАТО |
| Оборонный колледж | Рим, Италия | - развитие критического, творческого и стратегического мышления по вопросам, представляющих важность для НАТО;  - достижение многонационального консенсуса | - обучение старших курсов по вопросам трансатлантической безопасности;  - проведение исследований;  - поддержка взаимодействия между союзниками по НАТО |  |
| Академия связи и информации | Оэйраш, Португалия | - управление, координирование и предоставление обучения;  - поддержка стратегических, оперативных и деловых целей НАТО | - предоставление услуг по обучению для НАТО и союзников в сфере кибербезопасности  - обучение инновациям и помощь в модернизации методов и инфраструктуры, связанных с образовательным процессом | сотрудники из Португалии, Бельгии,  Нидерландов и Норвегии |

Источник: составлено автором на основе данных с официального сайта НАТО и его учреждений[[168]](#footnote-169).

Приложение 3

**Сравнительная таблица подходов ЕС и НАТО к политике кибербезопасности**

|  |  |  |
| --- | --- | --- |
|  | **Подход ЕС** | **Подход НАТО** |
| **Нормативно-правовая база** | 1. Стратегия кибербезопасности ЕС;  2. Директива по повышению безопасности сетей и информационных систем (NIS);  3.Закон о кибербезопасности;  4. План Европейской Комиссии по восстановлению Европы;  5. Стратегия Союза безопасности на 2020-2025 гг.;  6. Приоритеты Европейской Комиссии на 2019-2022 гг. | 1. Стратегическая концепция НАТО;  2. Таллиннское руководство по международному праву, применимому к кибернетическим войнам (Tallinn 2.0);  3. Комплексная политика киберзащиты (2021);  4. Программа развития Альянса «НАТО 2030» |
| **Институты и учреждения** | 1. Агентство по сетевой и информационно безопасности (ENISA);  2. Центр обмена и анализа информации (ISAC);  3. Объединенный исследовательский центр (JRC);  4. Национальные компетентные учреждения (CSIRT и CERT);  5. Европейская организация по кибербезопасности (ECSO);  6. Европейский центр по борьбе с киберпреступностью. | 1. Технический центр по реагированию на компьютерные инциденты (NCIRC);  2. Центр управления кибервойной (CDMA);  3. Центр передового опыта по совместной киберзащите (CCD COE);  4. Агентство связи и информации НАТО (NCIA);  5. Школа НАТО;  6. Академия связи и информации;  7. Оборонный колледж;  8. Национальные компетентные учреждения (CSIRT и CERT);  9. Центр киберопераций НАТО. |
| **Понимание кибербезопасности** | Кибербезопасность – это безопасность сетевых и информационных систем или глобальный подход на уровне Союза, охватывающий общие минимальные требования к наращиванию потенциала и планированию, обмену информацией, сотрудничеству и общим требованиям безопасности для операторов основных услуг и поставщиков цифровых услуг. | В дискурсе чаще встречается термин «киберзащита».  Киберзащита – это защита собственных сетей, работа в киберпространстве (в том числе в рамках операций и миссий Североатлантического Альянса), помощь союзникам в повышении их национальной устойчивости и предоставление платформы для политических консультаций и коллективных действий. |
| **Цели** | - повышение безопасности сетевых и информационных систем, включая определение высоких стандартов, разработку европейской киберзащиты, поддержку МСБ, привлечение специалистов и финансов;  - укрепление коллективных возможностей государств-членов и защита граждан и их интересов в киберпространстве;  - работа с внешними партнерами для обеспечения международной безопасности и стабильности | - укрепление единства, солидарности и сплоченности союзников, в том числе для усиления центральной роли трансатлантических связей;  - расширение политических консультаций и координации между союзниками по НАТО;  - усиление политической роли НАТО и соответствующих инструментов для противодействия текущим и будущим угрозам и вызовам Североатлантического Альянса;  - тесное сотрудничество с постоянно растущим кругом внешних партнеров |
| **Инструменты** | 1. Платформа динамического управления мультиоблачными приложениями (CyCLONe);  2. Постоянное структурированное сотрудничество по вопросам безопасности и обороны (PESCO);  3. Совместная группа по борьбе с киберпреступностью (J-CAT);  4. Horizon 2020, Horizon Europe;  5. Киберполигоны и моделирование киберугроз;  5. Инструментарий в области кибердипломатии | 1. Обязательства по киберзащите;  2. Группы быстрого реагирования (RRTs);  3. Киберполигон (Cyber Range) и учения Cyber Coalition;  4. Меморандум о взаимопонимании;  5. Промышленное  киберпартнерство;  6. Платформа обмена информацией о вредоносных программах НАТО. |
| **Действия** | - разработка общеевропейской системы сертификации;  - повышение ситуационной осведомленности через соответствующие Центры;  - определение общего понимания кибербезопасности, ее основных инструментов и механизмов;  - финансирование перспективных проектов через Фонды ЕС;  - проведение расследований, связанных с киберпреступностью;  - обучение в области ИКТ. | - создание и поддержание консультационных и командных сетей НАТО;  - проведение международных учений в киберпространстве;  - предоставление союзникам по НАТО необходимых инструментов и инфраструктуру для проведения операций в киберпространстве;  - проведение межнациональных программ обучения, которые охватывают гражданский и военный персонал. |
| **Перспективы развития** | 1. Обновление существующей Директивы NIS посредством расширения ее сферы действия;  2. Расширение практики проведения киберучений на существующих киберполигонах;  3. Поддержка цифровой стратегии ЕС через объединение имеющегося опыта и внедрение новейших технологий | 1. Укрепление потенциала защиты союзников по НАТО от гибридных и кибератак;  2. Повышение осведомленности о природе происхождения гибридных угроз и организованных преступных групп, стоящих за ними;  3. Финансирование, пополнение и обучение персонала новейшим способам киберзащиты;  4. Определение правовых и этических рамок для эффективных и законных действий в киберпространстве. |

Приложение 4

Источник: составлено автором.

Приложение 5

**Контент-анализ стратегических документов ЕС и НАТО в области кибербезопасности**

**Кодировальная матрица**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Тема** | | **Наличие тематического направления** | | | | | | | |
| **Стратегические документы ЕС** | | | **Стратегические документы НАТО** | | | **Совместные документы** |
| **Текст №1** | **Текст №2** | **Текст №3** | **Текст №4** | **Текст №5** | **Текст №6** | **Текст №7** | |
| **A** | a1 | **+** |  | **+** |  |  |  |  | |
| a2 | **+** |  |  | **+** |  |  | **+** | |
| a3 | **+** | **+** | **+** | **+** | **+** |  | **+** | |
| a4 | **+** | **+** |  |  |  |  |  | |
| a5 | **+** | **+** |  | **+** | **+** | **+** |  | |
| a6 | **+** |  | **+** |  | **+** | **+** | **+** | |
| a7 |  |  | **+** | **+** | **+** | **+** | **+** | |
| **B** | b1 | **+** |  | **+** |  |  | **+** | **+** | |
| b2 | **+** |  | **+** |  |  |  |  | |
| b3 | **+** |  |  |  |  |  |  | |
| b4 | **+** | **+** | **+** | **+** | **+** | **+** | **+** | |
| **C** | c1 | **+** | **+** | **+** | **+** |  | **+** |  | |
| c2 | **+** | **+** | **+** | **+** | **+** | **+** | **+** | |
| c3 | **+** | **+** |  |  |  | **+** | **+** | |
| **D** | d1 | **+** | **+** |  |  |  |  |  | |
| d2 |  | **+** |  |  |  |  |  | |
| d3 |  | **+** |  |  |  |  |  | |

**Результаты**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | a1 | a2 | a3 | a4 | a5 | a6 | a7 | b1 | b2 | b3 | b4 | c1 | c2 | c3 | d1 | d2 | d3 |
| **Только ЕС** | 2 |  |  | 2 |  |  |  |  | 2 | 1 |  |  |  | 2 | 2 | 1 | 1 |
| **Только НАТО** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Все** |  | 3 | 6 |  | 5 | 5 | 5 | 4 |  |  | 7 | 5 | 7 |  |  |  |  |

**Пояснение:**

Текст №1 – Стратегия кибербезопасности ЕС для цифрового десятилетия (2020 г.);

Текст №2 – Приоритеты Европейской Комиссии на 2019-2022 гг. (2019 г.);

Текст №3 – Стратегия Союза безопасности на 2020-2025 гг. (2020 г.);

Текст №4 – Стратегическая концепция НАТО (2010 г.);

Текст №5 – Обязательства по киберзащите(2016 г.)

Текст №6 – Программа развития Альянса «НАТО 2030» (2021 г.);

Текст №7 – Совместная декларация ЕС-НАТО (2018 г).

**Тематические направления:**

**A – Повышение кибербезопасности основных процессов и их составляющих:**

a1 – Пересмотр существующей нормативно-правовой базы;

a2 – Создание оперативных центров или специальных учреждений безопасности в государствах-членах;

a3 – Обеспечение высоких стандартов кибербезопасности всех объектов инфраструктуры;

a4 – Поддержка малого и среднего бизнеса, связанных с обеспечением кибербезопасности;

a5 – Привлечение специализированного персонала;

a6 – Инвестирование в обучение и инновации;

a7 – Повышение киберосведомленности посредством обмена опытом и информацией.

**B – Укрепление коллективного потенциала государств-членов для реагирования на** **крупные кибератаки:**

b1 – Создание общего киберподразделения как платформы для сотрудничества;

b2 – Комплексный подход для борьбы с киберпреступностью в рамках правоохранительной деятельности;

b3 – Использование дипломатических инструментов;

b4 – Повышение возможностей киберзащиты государств-членов.

**C – Создание глобального и открытого киберпространства:**

c1 – Подтверждение лидерства организации в рамках норм, стандартов и границ кибербезопасности;

c2 – Сотрудничество с партнерами и многосторонним сообществом заинтересованных акторов;

c3 – Углубление глобального потенциала и киберустойчивости посредством интеграции и защиты демократических систем.

**D – Поддержка гражданского общества в рамках обеспечения кибербезопасности:**

d1 –Защита цифровых прав граждан;

d2 – Обеспечение всеобщего доступа граждан к Интернету и его возможностям;

d3 – Содействие участию граждан в цифровом общественном пространстве.

Приложение 6

**Основные тенденции и влияющие на них факторы в трансатлантическом пространстве безопасности (ТПБ)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Тенденции** | Интеграция  ОПБО ЕС | Дезинтеграция  ОПБО ЕС | Консолидация государств ТПБ | Разногласия государств ТПБ | Институционализация в отношениях  ЕС и НАТО | Статус-кво в институтах ЕС и НАТО |
| **Факторы** | Межгосударственные противоречия | | Усиление роли РФ или КНР в регионе | | Политические разногласия государств | |
| Влияние третьих сторон (США, КНР, РФ) на страны ЕС | | Развитие ОПБО ЕС | | Заключение соглашения об обмене засекреченной информацией | |
| Определение стратегической автономии ЕС | | Дублирование функций между организациями | |
| Влияние ТНК на оборонно-промышленный комплекс и направления политики ЕС | | Роль США в политической и военной деятельности ЕС | | Развитие НАТО и ОПБО ЕС | |
| Урегулирование или замораживание конфликта на Украине | |
| Стабильность в соседних регионах | | Продолжение и еще большая эскалация конфликта на Украине | | Возникновение новых общих угроз | |
| **Глобальные факторы** | Обострение конфликта между США и КНР | | | | | |
| Изменение роли развивающихся стран в мировой экономике и технологиях | | | | | |
| Военно-технологические достижения мирового уровня | | | | | |
| Финансово-экономические и продовольственные кризисы | | | | | |
| Глубокий политический кризис в развитых странах мира | | | | | |
| Войны между великими державами | | | | | |
| Глобальные бедствия и пандемии | | | | | |
| Экологические катастрофы | | | | | |
| Доступ террористов к ОМУ | | | | | |

Источник: составлено автором.

**Сценарии развития отношений ЕС и НАТО и тенденции, оказывающие на них влияние**

|  |  |  |  |
| --- | --- | --- | --- |
| **Сценарии** | **Тенденции** | | |
| **Расширение сотрудничества** | Интеграция ОПБО ЕС | Консолидация государств ТПБ | Институционализация в отношениях  ЕС и НАТО |
| **Статус-кво в отношениях** | Интеграция ОПБО ЕС | Разногласия государств ТПБ | Статус-кво в институтах ЕС и НАТО |
| **Деградация сотрудничества** | Интеграция ОПБО ЕС | Разногласия государств ТПБ | Статус-кво в институтах ЕС и НАТО |
| Дезинтеграция ОПБО ЕС |

1. Hybrid threats as a concept // Hybrid CoE. URL: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> (дата обращения: 20.02.2022). [↑](#footnote-ref-2)
2. Walden I. Crime and Security in Cyberspace / I. Walden // Cambridge review of the International Affairs. – 2005. № 18(1). – P. 51–68; Clark D. Characterizing cyberspace: past, present and future / D. Clark // MIT CSAIL. 2010. URL: <https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf>; Fichtner L. What kind of cyber security? Theorizing cyber security and mapping approaches / L. Fichtner // Internet Policy Review. – 2019. №7 (2). – P. 1–19; Miron W. Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure / W. Miron, K. Muita // Technology Innovation Management Review. – 2014. – P. 33–39; Lezzi M. Cybersecurity for Industry 4.0 in the current literature: A reference framework / M. Lezzi, M. Lazoi, A. Corallo // Elsevier. Computers in Industry. – 2018. №103. – P. 97–110; Stevens T. Global Cybersecurity: New Directions in Theory and Methods / T. Stevens // Politics and Governance. – 2018. № 6(2). – P. 1–4; Carr M. Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance // M. Carr, F. Lesniewska. – 2020. № 34(3). – P. 391–412; Kerschischnig G. Cyberthreats and International Law / G. Kerschischnig – The Hague, 2012. – 386 p.; Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. №1 (2) – С. 22–27. [↑](#footnote-ref-3)
3. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты перспективы: дис. д. полит. наук: 23.00.04. – МГИМО МИД, Москва, 2017. – 332 с.; Чеботарева А.А. Научные подходы к определению понятия «информационная безопасность» / А.А. Чеботарева // Информационное право. – 2011. №1. – С. 3–6; Атаманов Г.А. Информационная безопасность: сущность и содержание / Г.А. Атаманов // Бизнес и безопасность в России. – 2007. №47. – С. 104–109; Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации: автореф. дис. канд. технич. Наук: 05.13.19. – СПбГУ ИТМО, Санкт-Петербург, 2008. – 145 с.; Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин. – СПб: Фонд Университет, 2000. – С. 51–57; Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» / А.А. Стрельцов // Информационное общество. – 2001. №. 4. – 52 с. [↑](#footnote-ref-4)
4. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. наук: 12.00.03. – Москва, 2016 – 66 с.; Кардава Н.В. Политика обеспечения кибербезопасности в Европейском Союзе: национальный и наднациональный уровни / Н.В. Кардава // Каспийский регион: политика, экономика, культура – 2019. № 3(60). – С. 73–78; Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. – 2017. № 6 – С. 44–51. [↑](#footnote-ref-5)
5. Hansen L. Digital Disaster, Cyber Security, and the Copenhagen School / L. Hensen, H. Nissenbaum // International Studies Quarterly. – 2015. №53. – P. 1155–1175; Gomez M.A. Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats // M.A. Gomez, C. Whyte // Oxford Academic. – 2021. № 4(65). – P. 1137–1150; Mitchell G. E. Correlates of State-Sponsored Cyber Conflict / G.E. Mitchell, A. Pytlak // Routledge Handbook of International Cybersecurity / eds. by T. Eneken, M. Kerttunen. – Oxford, UK: Routledge, 2020. – P. 22–36; Salminen M. The becoming of cyber-military capabilities / M. Salminen, M. Kerttunen // Routledge Handbook of International Cybersecurity / eds. by T. Eneken, M. Kerttunen. – Oxford, UK: Routledge, 2020. – P. 94–109; Паршин С. А. Кибервойны – реальная угроза национальной безопасности / С. А. Паршин, Ю. Е. Горбачев, Ю. А. Кожанов – М.: КРАСАНД, 2011. – 96 с.; Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев – М.: Харвест, 2004. – 426 с.; Макаров В.Е. Политические и социальные аспекты информационной безопасности: монография – Таганрог: Изд. С.А. Ступин, 2015. – 351 с.; Бухарин С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов – М.: Академический проект, 2007. – 382 с. [↑](#footnote-ref-6)
6. Angelov I. The Security Environment and the Challenges to the European Union and NATO in the field of Security / I. Angelov // Security & Future. – 2019. № 3(1). – P. 17–21; Simion E. NATO-EU Cooperation / E. Simion // International Conference KNOWLEDGE-BASED ORGANIZATION. – 2018. № 24(1). – P. 211–214; Græger N. Grasping the everyday and extraordinary in EU–NATO relations: The added value of practice approaches / N. Græger // European Security. – 2017. № 26(3). – P. 340–358; Biscop S. EU-U.S. Consensus and NATO-EU Cooperation / eds. by T. Valasek. – Brussels: Carnegie Endowment for International Peace, 2019. – P. 18. – URL: <https://carnegieendowment.org/files/NATO_int_final1.pdf>; Козубенко И.И. Институциональное взаимодействие структур ЕС и НАТО / И.И. Козубенко // Новое слово в науке: перспективы развития. – 2016. № 2 (8). – С. 39–42; Буденный А.А. НАТО и военно-политическая независимость Западной Европы / А.А. Буденный // США и Канада: экономика, политика, культура. – 2018. № 4. – С. 98–105. [↑](#footnote-ref-7)
7. Howorth J. The Euro-Atlantic Security Dilemma: France, Britain, and the ESDP / J. Howorth // Journal of Transatlantic Studies. – 2005. № 3(1). – P. 39–54; Howorth J. Strategic Autonomy and EU-NATO Cooperation: A Win-Win Approach / J. Howorth // L’Europe En Formation. – 2019. № 389(2). – P. 85–103; Howorth J. (2017). EU–NATO cooperation: The key to Europe’s security future / J. Howorth // European Security. – 2017. № 26(3). – P. 454–459; Posen B. R. ESDP and the structure of world power / B.R. Posen // The International Spectator. – 2004. № 39(1). – P. 5–17; Тузовская Н.Ю. Пределы «Стратегического партнерства» ЕС и НАТО / Н.Ю. Тузовская // Актуальные проблемы Европы. – 2010. – С. 93–94; Щербак И. Стратегическая автономия ЕС и проблемы формирования внешнеполитической повестки в эпоху пандемии / И. Щербак // Современная Европа. – 2020. №6. – С. 29–40; Стратегическая автономия ЕС и перспективы сотрудничества с Россией / под ред. Н.К. Арбатовой, А.М. Кокеева – М.: Весь мир, 2020. – 368 с. [↑](#footnote-ref-8)
8. Lete, B. EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions / B. Lete, P. Pernik // German Marshall Fund of the United States. – 2017. URL: https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions; Pernik P. Improving Cyber Security: NATO and the EU / P. Pernik // International Centre for Defence Studies. – 2014. – P. 17–25; Poptchev P. NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages / P. Poptchev // Information and Security. – 2020. № 45. – P. 35–55; Ilves L. K. European Union and NATO: Global Cybersecurity Challenges / L.K. Ilves, T.J. Evans, F.J. Cilluffo, A.A. Nadeau // PRISM. – 2016. № 2(6). – P. 126–141. [↑](#footnote-ref-9)
9. Kovacs L. Cyber Security Policy and Strategy in the European Union and NATO / L. Kovacs // Land Forces Academy Review. – 2018. № 1(89). – P. 16–24; Shopina I. Cybersecurity: legal and organizational support in leading countries, NATO and EU standards / I. Shopina, D. Khomiakov, N. Khrystynchenko, S. Zhukov, D. Shpenov // Journal of security and sustainability issues. – 2020. № 3(9). – P. 977–992; Шариков П. Подходы США, ЕС и России к проблеме информационной политики / П. Шариков, Н. Степанова // Современная Европа. – 2019.№2. – С. 73-83. [↑](#footnote-ref-10)
10. Calderoni F. The European legal framework on cybercrime: striving for an effective implementation / F. Calderoni // Crime Law Soc Change. – 2010. №54. – P. 339–357; Christou G. The challenges of cybercrime governance in the European Union / G. Christou // European Politics and Society. – 2018. – P. 1–21; Fuster G.G. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights // G.G. Fuster, L. Jasmontaite // The Ethics of Cybersecurity. – 2020. – P. 97–115; Кардава Н. В. Политика обеспечения безопасности в Европейском Союзе: национальный и наднациональный уровни / Н. В. Кардава // THE CASPIAN REGION: Politics, Economics, Culture. – 2019. № 3(60). – С. 73–76; Пантин В.И. Кибербезопаность: проблемы формирования единой политики в Европейском Союзе / В.И. Пантин, Н.В. Кардава, // Вестник Пермского университета. Политология. – 2018. №3. – С. 5–18. [↑](#footnote-ref-11)
11. McGee J. NATO and Cyber Defense: A Brief Overview and Recent Events / J. McGee. – 2011. URL: <https://www.csis.org/blog/natoand-cyber-defense-brief-overview-and-recentevents>; Hughes R.B. NATO and Cyber Security: Mission accomplished? / R.B. Hughes // Charlise. – 2016. URL: http://www.carlisle.army.mil/ DIME/documents/ NATO%20 and%20 Cyber%20Defence.pdf; Goldgeier J. The Future of NATO. NATO Science for Peace and Security Series / J. Goldgeier // Human and Societal Dynamics. IOS Press. – 2011. №76. – P. 1–12; Kempf A. Considerations for NATO Strategy on Collective Cyber Defense / A. Kempf. – 2018. URL: http://csis.org/ blog /considerations-nato-strategy-collective-cyberdefens; Манойло А.В. Современные стратегии кибербезопасности и киберобороны НАТО / А.В. Манойло // Актуальные проблемы Европы. – 2020. №3. – С. 160–184; Шариков П.А. Военные аспекты кибербезопасности в контексте

    специальной военной операции РФ на территории Украины / П.А. Шариков // Аналитические записки Института Европы РАН. Выпуск II. – 2022, № 13(280). – С. 5–12; Казаковцев А.В. НАТО и кибербезопасность / А.В. Казаковцев // Вестник Волгоградского гос. ун-та. – 2012. № 2(22). – С. 109–114; Курылев К.Л. Цифровая зависимость НАТО / К.Л. Курылев, В.Т. Цаканян // Вестник Моск. гос. областного ун-та. Серия: История и политические науки. – 2018. №1. – С. 45–53. [↑](#footnote-ref-12)
12. Buzan B. Security: A New Framework for Analysis. Boulder / B. Buzan, O. Wæver, J. De Wilde. – CO: Lynne Rienner Publishers, 1998. – 239 p. [↑](#footnote-ref-13)
13. Прохоренко И.Л. Пространственный подход в исследовании международных отношений / И.Л. Прохоренко. – М.: ИМЭМО РАН, 2015. – 111 с. [↑](#footnote-ref-14)
14. Богданов А.А. Тектология: всеобщая организационная наука / А.А. Богданов. – М., 1989. – URL: <https://gtmarket.ru/library/basis/5909> (дата обращения: 15.02.2022). [↑](#footnote-ref-15)
15. Hall P.A. Political Science and Three New Institutionalisms / P.A. Hall, R.C.R. Taylor // MPIFG Discussion Paper. – 1996. – 32 p. [↑](#footnote-ref-16)
16. The EU’s Cybersecurity Strategy for the Digital Decade // European Commission. – Brussels, 16.12.2020, JOIN (2020) 18. URL: <file:///C:/Users/%D0%B0%D1%81%D1%83%D1%81/Downloads/join2020_18_en_act_part1_v9_-_copy_2DD42D12-B246-B9BE-E927D92051AE4753_72164.pdf>; 6 Commission priorities for 2019-24 // European Commission. URL: <https://ec.europa.eu/info/strategy/priorities-2019-2024_en>; Communication from the Commission on the EU Security Union Strategy // European Commission. Brussels, 24.7.2020, COM (2020) 605. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605>; Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon // NATO. 19.11.2010. URL: <https://www.nato.int/cps/en/natohq/official_texts_68580.htm>; Cyber Defence Pledge // NATO. – Press Release (2016) 124, 8.7.2016. URL: <https://www.nato.int/cps/en/natohq/official_texts_133177.htm>; Brussels Summit Communiqué // NATO. – Press Release (2021) 086. 14.6.2021. URL: <https://www.nato.int/cps/en/natohq/news_185000.htm>; Europe 2020: a strategy for smart, sustainable and inclusive growth // European Commission. – Brussels, 3.3.2010, COM (2010) 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC2020&from=en. [↑](#footnote-ref-17)
17. The North Atlantic Treaty // NATO. – Washington D.C. 4.04.1949. URL: https://www.nato.int/cps/en/natolive/official\_texts\_17120.htm. [↑](#footnote-ref-18)
18. Consolidated Version of the Treaty on European Union // Official Journal of the European Union. 7.6.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016M/TXT&from=EN. [↑](#footnote-ref-19)
19. Consolidated Version of the Treaty on the Functioning of the European Union // Official Journal of the European Union. 26.10.2012. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN. [↑](#footnote-ref-20)
20. Treaty of Lisbon // Official Journal of the European Union. 17.12.2007. URL: http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC\_19. [↑](#footnote-ref-21)
21. A Digital Agenda for Europe // European Commission. – Brussels, 19.5.2010, COM (2010)245. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>; Combatting Fraud and Counterfeiting of Non-Cash Means of Payment // European Commission. URL: <https://ec.europa.eu/home-affairs/pages/page/combatting-fraud-and-counterfeiting-non-cash-means-payment_en>; Defending the networks: the NATO Policy on Cyber Defence // NATO. 19.8.2011. URL: <https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf>; Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”) // Council of the European Union. – Brussels, 7.6.2017, 9916/17. URL: <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>; ENISA Mandate and Regulatory Framework // ENISA. URL: <https://www.enisa.europa.eu/about-enisa/regulatory-framework>; EU cybersecurity initiatives: working towards a more secure online environment, Factsheet // European Commission. 01.2017. URL: <https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf>; Memorandum of understanding // NATO, 3.11.2008. URL: <https://www.nato.int/cps/en/natohq/official_texts_18839.htm?selectedLocale=en>; On Critical Information Infrastructure Protection “Achievements and next steps: towards global cyber-security” // European Commission. – Brussels, 31.3.2011, COM (2011) 163. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF>; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // Official Journal of the European Union. – 7.6.2019, L 151/15. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC>; Resilience, Deterrence and Defence: Building strong cybersecurity for the EU // European Commission and High Representative of the Union for Foreign Affairs and Security Policy. – Brussels, 13.9.2017, JOIN (2017) 450. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en>. [↑](#footnote-ref-22)
22. Brussels Summit Communiqué // NATO. – Press Release (2021) 086. 14.6.2021. URL: <https://www.nato.int/cps/en/natohq/news_185000.htm>; Lisbon Summit Declaration issued by the Heads of state and Government participating in the meeting of the North Atlantic Council in Lisbon // NATO. – Press Release (2010) 155, 20.11.2010. URL: <https://www.nato.int/cps/em/natohq/official_texts_68828.htm>; Prague Summit Declaration // NATO. – Press Release (2002) 127. 21.11.2002. URL: <https://www.nato.int/cps/en/natohq/official_texts_19552.htm>; [↑](#footnote-ref-23)
23. Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization // NATO. – Press Release (2017) 174. 5.12.2017. URL: <https://www.nato.int/cps/en/natohq/official_texts_149522.htm>; Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 16.06.2020. URL: <https://www.consilium.europa.eu/media/44451/200616-progress-report-nr5-eu-nato-eng.pdf>; Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017 // NATO. 17.06.2019. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf>; oint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO // NATO. – Press Release (2016) 119. 8.07.2016. URL: <https://www.nato.int/cps/en/natohq/official_texts_133163.htm>; Joint declaration on EU-NATO cooperation by President of the European Council, President of the European Commission, and Secretary General of NATO // European Council. Council of the European Union. – Press Release. 10.07.2018. URL: <https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf>; Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 3.06.2021. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf>; Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 8.06.2018. – P. 4. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf>. [↑](#footnote-ref-24)
24. CCDEOE official page. URL: <https://ccdcoe.org/history.html>; Cyber Threats and Incident Response Information Sharing Platform (CTIRISP) // PESCO Projects. URL: <https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/>; Cybersecurity Policies // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq8796b>; CyCLONe official page. URL: <https://www.cyclone-project.eu/>; EC3 official page. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>; ENISA official page. URL: <https://www.enisa.europa.eu/about-enisa>; Joint Cybercrime Action Taskforce (J-CAT) // Europol. URL: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce>; NATO Allies and partners participate in large-scale cyber defence exercise // NATO. – News. 29.4.2022. URL: <https://www.nato.int/cps/en/natohq/news_194902.htm?selectedLocale=en>; NATO and the European Union enhance cyber defence cooperation // NATO. – News. 10.02.2016.URL: <https://www.nato.int/cps/en/natohq/news_127836.htm?selectedLocale=en>; NATO presents the Agenda for 2030 // European Commission. – News. 9.6.2021. URL: <https://ec.europa.eu/newsroom/cipr/items/713800/en>; NCI Agency official page. URL: <https://www.ncia.nato.int/>; NDS official page. URL: https://www.ndc.nato.int/; NCI Academy // Agency NCI. URL: <https://www.ncia.nato.int/what-we-do/nci-academy.html>; NSO official page. URL: <https://www.natoschool.nato.int/>. [↑](#footnote-ref-25)
25. Приложение 5. [↑](#footnote-ref-26)
26. Кинаш Е.И. Политика обеспечения информационной безопасности ЕС: основные проблемы и вызовы / Кинаш Е.И. // Сборник материалов II научной конференции студентов и молодых ученых «Orbes Politici». – 2022. №1. – С. 43– 44; Kinash E. Wittmann V. Science Diplomacy for Environment: Global Outlooks and Green Digital Diplomacy as a New Approach in the EU Environmental Diplomacy / E. Kinash, V. Wittman // Russian political science. – 2022. №21. – 24–34. [↑](#footnote-ref-27)
27. List of data breaches in 2021 // IT Governance. URL: <file:///C:/Users/%D0%B0%D1%81%D1%83%D1%81/Downloads/2021_data_breach_infographic.pdf> (дата обращения: 10.02.2022). [↑](#footnote-ref-28)
28. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев – М.: Харвест, 2004. – 426 с. [↑](#footnote-ref-29)
29. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. – 2017. № 6 – С. 45. [↑](#footnote-ref-30)
30. Oxford Online Dictionary // Oxford: Oxford University Press. URL: <http://www.oxforddictionaries.com/definition/english/Cybersecurity> (дата обращения: 10.02.2022). [↑](#footnote-ref-31)
31. Gibson W. Neuromancer / W. Gibson. – Orion Publishing Group, 2016. – 314 p. [↑](#footnote-ref-32)
32. Clark D. Characterizing cyberspace: past, present and future / D. Clark // MIT CSAIL. 2010. URL: https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf (дата обращения: 10.02.2022). [↑](#footnote-ref-33)
33. Buzan B. Security: A New Framework for Analysis. Boulder / B. Buzan, O. Wæver, J. De Wilde. – CO: Lynne Rienner Publishers, 1998. – 239 p. [↑](#footnote-ref-34)
34. Fichtner L. What kind of cyber security? Theorizing cyber security and mapping approaches / L. Fichtner // Internet Policy Review. – 2019. №7 (2). – P. 9. [↑](#footnote-ref-35)
35. Digital Millennium Copyright Act // U.S. Copyright Office Summary. 12.1998. URL: <https://www.copyright.gov/legislation/dmca.pdf> (дата обращения: 10.02.2022). [↑](#footnote-ref-36)
36. Doctorow C. America’s broken digital copyright law is about to be challenged in court / C. Doctorow // The Guardian. 21.07.2016. URL: <https://www.theguardian.com/technology/2016/jul/21/digital-millennium-copyright-act-eff-supreme-court> (дата обращения: 10.02.2022). [↑](#footnote-ref-37)
37. What is Stuxnet? // Trellix. URL: <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html> (дата обращения: 10.02.2022). [↑](#footnote-ref-38)
38. Fichtner L. What kind of cyber security? Theorizing cyber security and mapping approaches / L. Fichtner // Internet Policy Review. – 2019. №7 (2). – P. 11. [↑](#footnote-ref-39)
39. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты перспективы: дис. д. полит. наук: 23.00.04. – МГИМО МИД, Москва, 2017. – С. 98. [↑](#footnote-ref-40)
40. Swedish National Cyber Security Strategy // Government offices of Sweden. 22.06.2017. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy (дата обращения: 10.02.2022). [↑](#footnote-ref-41)
41. German National Cyber Security Strategy // Federal Ministry of the Interior. 09.09.2021. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany (дата обращения: 10.02.2022). [↑](#footnote-ref-42)
42. Stevens T. Global Cybersecurity: New Directions in Theory and Methods / T. Stevens // Politics and Governance. – 2018. № 6(2). – P. 1. [↑](#footnote-ref-43)
43. Gomez M.A. Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats // M.A. Gomez, C. Whyte // Oxford Academic. – 2021. № 4(65). – P. 1137–1150. [↑](#footnote-ref-44)
44. Чеботарева А.А. Научные подходы к определению понятия «информационная безопасность» / А.А. Чеботарева // Информационное право. – 2011. №1. – С. 3–6. [↑](#footnote-ref-45)
45. Атаманов Г.А. Информационная безопасность: сущность и содержание / Г.А. Атаманов // Бизнес и безопасность в России. – 2007. №47. – С. 108. [↑](#footnote-ref-46)
46. Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации: автореф. дис. канд. технич. Наук: 05.13.19. – СПбГУ ИТМО, Санкт-Петербург, 2008. – С. 34. [↑](#footnote-ref-47)
47. Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. №1 (2) – С. 26. [↑](#footnote-ref-48)
48. Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин. – СПб: Фонд Университет, 2000. – С. 428. [↑](#footnote-ref-49)
49. Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» / А.А. Стрельцов // Информационное общество. – 2001. №. 4. – С. 16. [↑](#footnote-ref-50)
50. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ // Консультант Плюс. URL: <http://www.consultant.ru/document/cons_doc_LAW_61798/> (дата обращения: 10.02.2022). [↑](#footnote-ref-51)
51. Pernik P. Improving Cyber Security: NATO and the EU / P. Pernik // International center for defense studies. – 2014. – P. 12. [↑](#footnote-ref-52)
52. Там же – P. 1. [↑](#footnote-ref-53)
53. Walden I. Crime and Security in Cyberspace / I. Walden // Cambridge review of the International Affairs. – 2005. № 18(1). – P. 51–68. [↑](#footnote-ref-54)
54. Howorth J. The Euro-Atlantic Security Dilemma: France, Britain, and the ESDP / J. Howorth // Journal of Transatlantic Studies. – 2005. № 3(1). – P. 39–54. [↑](#footnote-ref-55)
55. Howorth J. Strategic Autonomy and EU-NATO Cooperation: A Win-Win Approach / J. Howorth // L’Europe En Formation. – 2019. № 389(2). – P. 85–103. [↑](#footnote-ref-56)
56. Posen B. R. ESDP and the structure of world power / B.R. Posen // The International Spectator. – 2004. № 39(1). – P. 5–17. [↑](#footnote-ref-57)
57. Howorth J. EU–NATO cooperation: The key to Europe’s security future / J. Howorth // European Security. – 2017. № 26(3). – P. 454–459. [↑](#footnote-ref-58)
58. Тузовская Н.Ю. Пределы «Стратегического партнерства» ЕС и НАТО / Н.Ю. Тузовская // Актуальные проблемы Европы. – 2010. – С. 93-94. [↑](#footnote-ref-59)
59. Щербак И. Стратегическая автономия ЕС и проблемы формирования внешнеполитической повестки в эпоху пандемии / И. Щербак // Современная Европа. – 2020. №6. – С. 29-40. [↑](#footnote-ref-60)
60. Стратегическая автономия ЕС и перспективы сотрудничества с Россией / под ред. Н.К. Арбатовой, А.М. Кокеева – М.: Весь мир, 2020. – 368 с. [↑](#footnote-ref-61)
61. Angelov I. The Security Environment and the Challenges to the European Union and NATO in the field of Security / I. Angelov // Security & Future. – 2019. № 3(1). – P. 17–21. [↑](#footnote-ref-62)
62. Simion E. NATO-EU Cooperation / E. Simion // International Conference KNOWLEDGE-BASED ORGANIZATION. – 2018. № 24(1). – P. 211–214. [↑](#footnote-ref-63)
63. Græger N. Grasping the everyday and extraordinary in EU–NATO relations: The added value of practice approaches / N. Græger // European Security. – 2017. № 26(3). – P. 340–358. [↑](#footnote-ref-64)
64. Biscop S. EU-U.S. Consensus and NATO-EU Cooperation / eds. by T. Valasek. – Brussels: Carnegie Endowment for International Peace, 2019. – P. 18. – URL: <https://carnegieendowment.org/files/NATO_int_final1.pdf> (дата обращения 15.02.2022). [↑](#footnote-ref-65)
65. Козубенко И.И. Институциональное взаимодействие структур ЕС и НАТО / И.И. Козубенко // Новое слово в науке: перспективы развития. – 2016. № 2 (8). – С. 39-42. [↑](#footnote-ref-66)
66. Буденный А.А. НАТО и военно-политическая независимость Западной Европы / А.А. Буденный // США и Канада: экономика, политика, культура. – 2018. № 4. – С. 98–105. [↑](#footnote-ref-67)
67. Kovacs L. Cyber Security Policy and Strategy in the European Union and NATO / L. Kovacs // Land Forces Academy Review. – 2018. № 1(89). – P. 18. [↑](#footnote-ref-68)
68. Lete, B. EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions / B. Lete, P. Pernik // German Marshall Fund of the United States. – 2017. URL: <https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions> (дата обращения: 15.02.2022). [↑](#footnote-ref-69)
69. Pernik P. Improving Cyber Security: NATO and the EU / P. Pernik // International Centre for Defence Studies. – 2014. – P. 20. [↑](#footnote-ref-70)
70. Poptchev P. NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages / P. Poptchev // Information and Security. – 2020. № 45. – P. 36. [↑](#footnote-ref-71)
71. Шариков П. Подходы США, ЕС и России к проблеме информационной политики / П. Шариков, Н. Степанова // Современная Европа. – 2019.№2. – С. 73-83. [↑](#footnote-ref-72)
72. Кардава Н. В. Политика обеспечения безопасности в Европейском Союзе: национальный и наднациональный уровни / Н. В. Кардава // THE CASPIAN REGION: Politics, Economics, Culture. – 2019. №3(60). – С. 76. [↑](#footnote-ref-73)
73. Прохоренко И.Л. Пространственный подход в исследовании международных отношений / И.Л. Прохоренко. – М.: ИМЭМО РАН, 2015. – 111 с. [↑](#footnote-ref-74)
74. Косолапов Н.А. Транснациональные политические пространства: явление и практика / Н.А., Косолапов, М.В. Стрежнева, И.Л. Прохоренко, Ф.Г. Войтоловский. – М: Весь мир, 2011. – С. 44. [↑](#footnote-ref-75)
75. Kaplan M.A. System and Process in International Politics / M.A. Kaplan. – Colchester: ECPR, 2005. – 260 p. [↑](#footnote-ref-76)
76. Easton. D. The Political System. An Inquiry into the State of Political Science / D. Easton. – N.Y.: Knopf, 1953. – 177 p. [↑](#footnote-ref-77)
77. Богатуров А.Д. Очерки теории и методологии политического анализа международных отношений / А.Д. Богатуров, Н.А. Косолапов, М.А, Хрусталев. – М.: НОФМО, 2002. – 390 с. [↑](#footnote-ref-78)
78. Богданов А.А. Тектология: всеобщая организационная наука / А.А. Богданов. – М., 1989. – URL: <https://gtmarket.ru/library/basis/5909> (дата обращения: 15.02.2022). [↑](#footnote-ref-79)
79. Guy P. B. Institutional Theory in Political Science / P.B. Guy. London: Pinter, 1999. – P. 40. [↑](#footnote-ref-80)
80. Hall P.A. Political Science and Three New Institutionalisms / P.A. Hall, R.C.R. Taylor // MPIFG Discussion Paper. – 1996. – 32 p. [↑](#footnote-ref-81)
81. Там же – 32 p. [↑](#footnote-ref-82)
82. Wind M. Sovereignty and European Integration: Towards a Post Hobbesian Order / M. Wind. – Palgrave, 2001. – Pp. 40–42. [↑](#footnote-ref-83)
83. Smith M. E. Europe’s Foreign and Security Policy: The Institutionalisation of Cooperation / M.E. Smith. –Cambridge: Cambridge University Steven, 2004 – P. 29. [↑](#footnote-ref-84)
84. Warleigh A. Influence and interest in the European Union: the new politics of persuasion and advocacy / A. Warleigh. – London: Europa Publications, 2002. – P. 9. [↑](#footnote-ref-85)
85. Wind M. Sovereignty and European Integration: Towards a Post Hobbesian Order / M. Wind. – Palgrave, 2001. – Pp. 40–42. [↑](#footnote-ref-86)
86. EU cybersecurity initiatives: working towards a more secure online environment, Factsheet // European Commission. 01.2017. URL: <https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf> (дата обращения: 20.03.2022). [↑](#footnote-ref-87)
87. A Digital Agenda for Europe // European Commission. – Brussels, 19.5.2010, COM (2010)245. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> (дата обращения: 20.03.2022). [↑](#footnote-ref-88)
88. Europe 2020: a strategy for smart, sustainable and inclusive growth // European Commission. – Brussels, 3.3.2010, COM (2010) 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC2020&from=en (дата обращения: 20.03.2022). [↑](#footnote-ref-89)
89. On Critical Information Infrastructure Protection “Achievements and next steps: towards global cyber-security” // European Commission. – Brussels, 31.3.2011, COM (2011) 163. URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF> (дата обращения: 20.03.2022). [↑](#footnote-ref-90)
90. Christou G. The EU's Approach to Cyber Security / G. Christou // EUSC Policy paper series. – Warwick, 2014. – P. 1–13. [↑](#footnote-ref-91)
91. Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace // European Commission. – Brussels, 7.2.2013, JOIN (2013) 1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN> (дата обращения: 20.03.2022). [↑](#footnote-ref-92)
92. The European Agenda on Security // European Commission. – Brussels, 28.4.2015, COM (2015) 185. URL: https://ec.europa.eu/home-affairs/system/files/2020-09/eu\_agenda\_on\_security\_en\_0.pdf (дата обращения: 20.03.2022). [↑](#footnote-ref-93)
93. A Digital Single Market Strategy for Europe // European Commission. – Brussels, 6.5.2015, COM (2015) 192. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> (дата обращения: 20.03.2022). [↑](#footnote-ref-94)
94. Strengthening Europe Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry // European Commission. – Brussels, 5.7.2016, COM (2016) 410. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=EN (дата обращения: 20.03.2022). [↑](#footnote-ref-95)
95. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, July 6 2016 // Official Journal of the European Union. – 19.7.2016, L 194/1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1> (дата обращения: 20.03.2022). [↑](#footnote-ref-96)
96. Combatting Fraud and Counterfeiting of Non-Cash Means of Payment // European Commission. URL: <https://ec.europa.eu/home-affairs/pages/page/combatting-fraud-and-counterfeiting-non-cash-means-payment_en> EN (дата обращения: 20.03.2022). [↑](#footnote-ref-97)
97. Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing of 13 December 2011 // Official Journal of the European Union. – 17.12.2011, L 335/1. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093> (дата обращения: 20.03.2022). [↑](#footnote-ref-98)
98. Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision of 12 August 2013 // Official Journal of the European Union. – 14.8.2013, L 218/8. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040> (дата обращения: 20.03.2022). [↑](#footnote-ref-99)
99. A Global Strategy for the European Union’s Foreign and Security Policy. Shared Vision, Common Action: A Stronger Europe // Council of the European Union. – Brussels, 14.11.2016. URL: <https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en> (дата обращения: 20.03.2022). [↑](#footnote-ref-100)
100. Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”) // Council of the European Union. – Brussels, 7.6.2017, 9916/17. URL: <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (дата обращения: 20.03.2022). [↑](#footnote-ref-101)
101. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU // European Commission and High Representative of the Union for Foreign Affairs and Security Policy. – Brussels, 13.9.2017, JOIN (2017) 450. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en (дата обращения 20.03.2022). [↑](#footnote-ref-102)
102. The Cybersecurity Strategy // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy> (дата обращения 20.03.2022). [↑](#footnote-ref-103)
103. A Europe fit for the digital age // The European Commission’s priorities. – European Commission, 2019. URL: <https://ec.europa.eu/info/strategy/priorities-2019-2024_en> (дата обращения: 20.03.2022). [↑](#footnote-ref-104)
104. ENISA Mandate and Regulatory Framework // ENISA. URL: <https://www.enisa.europa.eu/about-enisa/regulatory-framework> (дата обращения: 20.03.2022). [↑](#footnote-ref-105)
105. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // Official Journal of the European Union. – 7.6.2019, L 151/15. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC> (дата обращения: 20.03.2022). [↑](#footnote-ref-106)
106. The European Cybersecurity Certification Group // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group> (дата обращения: 20.03.2022). [↑](#footnote-ref-107)
107. Cybersecurity Policies // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq8796b> (дата обращения: 20.03.2022). [↑](#footnote-ref-108)
108. CyCLONe official page. URL: <https://www.cyclone-project.eu/> (дата обращения: 20.03.2022). [↑](#footnote-ref-109)
109. Permanent Structured Cooperation (PESCO) official page. URL: <https://www.pesco.europa.eu/> (дата обращения: 20.03.2022). [↑](#footnote-ref-110)
110. PESCO: EU paves way to defense union // Deutsche Welle. 13.11.2017. URL: <https://www.dw.com/en/pesco-eu-paves-way-to-defense-union/a-41360236> (дата обращения 20.03.2022). [↑](#footnote-ref-111)
111. EC3 official page. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения 20.03.2022). [↑](#footnote-ref-112)
112. Joint Cybercrime Action Taskforce (J-CAT) // Europol. URL: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce> (дата обращения: 05.05.2022). [↑](#footnote-ref-113)
113. Law enforcement agencies across the EU prepare for major cross-border cyber-attacks // Europol. – News, 18.03.2019. URL: <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks> (дата обращения: 20.03.2022). [↑](#footnote-ref-114)
114. Proposal for directive on measures for high common level of cybersecurity across the Union // European Commission. – 16.12.2020. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union> (дата обращения: 20.03.2022). [↑](#footnote-ref-115)
115. Приложение 1. [↑](#footnote-ref-116)
116. Healey J. NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow / J. Healey. K. T. Jordan // Atlantic Council. 9.2014. – P. 1. URL: <https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf> (дата обращения: 15.03.2022). [↑](#footnote-ref-117)
117. Prague Summit Declaration // NATO. – Press Release (2002) 127. 21.11.2002. URL: <https://www.nato.int/cps/en/natohq/official_texts_19552.htm> (дата обращения: 15.03.2022). [↑](#footnote-ref-118)
118. Healey J. Op. sit. – P. 2. [↑](#footnote-ref-119)
119. Bucharest Summit declaration // NATO. – Press Release (2008) 049. 3.4.2008. URL: <https://www.nato.int/cps/us/natohq/official_texts_8443.htm> (дата обращения: 15.03.2022). [↑](#footnote-ref-120)
120. Healey J. Op. sit. – P. 3. [↑](#footnote-ref-121)
121. CCDEOE official page. URL: <https://ccdcoe.org/history.html> (дата обращения: 15.03.2022). [↑](#footnote-ref-122)
122. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon // NATO. 19.11.2010. URL: <https://www.nato.int/cps/en/natohq/official_texts_68580.htm> (дата обращения: 15.03.2022). [↑](#footnote-ref-123)
123. Lisbon Summit Declaration issued by the Heads of state and Government participating in the meeting of the North Atlantic Council in Lisbon // NATO. – Press Release (2010) 155, 20.11.2010. URL: <https://www.nato.int/cps/em/natohq/official_texts_68828.htm> (дата обращения 15.03.2022). [↑](#footnote-ref-124)
124. Defending the networks: the NATO Policy on Cyber Defence // NATO. 19.8.2011. URL: <https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf> (дата обращения 15.03.2022). [↑](#footnote-ref-125)
125. Cyber Defence Pledge // NATO. – Press Release (2016) 124, 8.7.2016. URL: <https://www.nato.int/cps/en/natohq/official_texts_133177.htm> (дата обращения 15.03.2022). [↑](#footnote-ref-126)
126. Cyber Defence // NATO. 23.3.2022. URL: <http://www.nato.int/cps/en/natohq/topics_78170.htm> (дата обращения 15.03.2022). [↑](#footnote-ref-127)
127. Schmitt M. N. Tallinn Manual on the International Law Applicable to Cyber Warfare / M.N. Schmitt. – UK: Cambridge University Press, 2013. – 215 p.; Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M.N. Schmitt. – UK: Cambridge University Press, 2017. – 569 p. [↑](#footnote-ref-128)
128. NATO Allies and partners participate in large-scale cyber defence exercise // NATO. – News. 29.4.2022. URL: <https://www.nato.int/cps/en/natohq/news_194902.htm?selectedLocale=en> (дата обращения: 15.03.2022). [↑](#footnote-ref-129)
129. NATO Cyber Defence, Factsheet // NATO, 4.2017. URL: https://www.nato.int/nato\_static\_fl2014/assets/pdf/pdf\_ 2018\_02/20180213\_1802-factsheet-cyber-defence-en.pdf (дата обращения: 15.03.2022). [↑](#footnote-ref-130)
130. NATO's Cyber Security Centre // NATO Communications and Information Agency. URL: <https://www.ncia.nato.int/what-we-do/cyber-security.html> (дата обращения: 15.03.2022). [↑](#footnote-ref-131)
131. CCD CE official page. URL: <https://ccdcoe.org/about-us/> (дата обращения: 15.03.2022). [↑](#footnote-ref-132)
132. Memorandum of understanding // NATO, 3.11.2008. URL: <https://www.nato.int/cps/en/natohq/official_texts_18839.htm?selectedLocale=en> (дата обращения: 15.03.2022). [↑](#footnote-ref-133)
133. Sharing malware information to defeat cyber attacks // NATO, 29.11.2013. URL: <https://www.nato.int/cps/en/natolive/news_105485.htm> (дата обращения: 15.03.2022). [↑](#footnote-ref-134)
134. NATO Cyber Defence, Factsheet // NATO, 2.2019. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf> (дата обращения: 15.03.2022). [↑](#footnote-ref-135)
135. NATO presents the Agenda for 2030 // European Commission. – News. 9.6.2021. URL: <https://ec.europa.eu/newsroom/cipr/items/713800/en> (дата обращения: 15.03.2022). [↑](#footnote-ref-136)
136. NATO 2030: United for a New Era // NATO Defense College. 25.11.2020. – P. 45. URL: <file:///C:/Users/%D0%B0%D1%81%D1%83%D1%81/Downloads/201201reflectiongroupfinalreportuni_01AA68FEB78CE059F77DA9F2DD4BFC98_75365_wfOiUrW14oBjHRPNn7tVylgBaI_76960.pdf> (дата обращения: 15.03.2022). [↑](#footnote-ref-137)
137. Там же. – P. 46. [↑](#footnote-ref-138)
138. Brussels Summit Communiqué // NATO. – Press Release (2021) 086. 14.6.2021. URL: <https://www.nato.int/cps/en/natohq/news_185000.htm> (дата обращения 15.03.2022). [↑](#footnote-ref-139)
139. Приложение 2. [↑](#footnote-ref-140)
140. Приложение 3. [↑](#footnote-ref-141)
141. Lisbon Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon // NATO. – Press Release (210) 155. 20.11.2010. URL: <https://www.nato.int/cps/en/natolive/official_texts_68828.htm> (дата обращения: 11.05.2022). [↑](#footnote-ref-142)
142. Helwig N. New Tasks for EU-NATO Cooperation An Inclusive EU Defence Policy Requires Close Collaboration with NATO / N. Helwig // German Institute for International and Security Affairs. – 2018. – P. 2. [↑](#footnote-ref-143)
143. Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO // NATO. – Press Release (2016) 119. 8.07.2016. URL: <https://www.nato.int/cps/en/natohq/official_texts_133163.htm> (дата обращения: 11.05.2022). [↑](#footnote-ref-144)
144. Joint declaration on EU-NATO cooperation by President of the European Council, President of the European Commission, and Secretary General of NATO // European Council. Council of the European Union. – Press Release. 10.07.2018. URL: <https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-145)
145. Simon J. S. The Father, the Son and the Holy Ghost: a Grounded Theory Approach to the Comparative Study of Decision-Making in the NAC and PSC // J. S. Simon, T. Nikola, G. Carmen // European Security. – 2017. № 3(26). – P. 359–379. [↑](#footnote-ref-146)
146. Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 8.06.2018. – P. 4. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-147)
147. Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 8.06.2018. – P. 2. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-148)
148. NATO and the European Union enhance cyber defence cooperation // NATO. – News. 10.02.2016.URL: <https://www.nato.int/cps/en/natohq/news_127836.htm?selectedLocale=en> (дата обращения: 11.05.2022). [↑](#footnote-ref-149)
149. Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization // NATO. – Press Release (2017) 174. 5.12.2017. URL: <https://www.nato.int/cps/en/natohq/official_texts_149522.htm> (дата обращения: 11.05.2022). [↑](#footnote-ref-150)
150. Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 8.06.2018. – P. 2. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-151)
151. Ibid. [↑](#footnote-ref-152)
152. Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017 // NATO. 17.06.2019. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-153)
153. Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 16.06.2020. URL: <https://www.consilium.europa.eu/media/44451/200616-progress-report-nr5-eu-nato-eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-154)
154. Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 3.06.2021. URL: <https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf> (дата обращения: 11.05.2022). [↑](#footnote-ref-155)
155. Приложение 4. [↑](#footnote-ref-156)
156. Light M. US and European perspectives on Russia / M. Light / eds. by J. Peterson, M. A. Pollack. Europe, America, Bush: Transatlantic relations in the twenty-first century. – London: Routledge. 2003. – P. 69. [↑](#footnote-ref-157)
157. Helwig N. New Tasks for EU-NATO Cooperation An Inclusive EU Defence Policy Requires Close Collaboration with NATO / N. Helwig // German Institute for International and Security Affairs. – 2018. – P. 3. [↑](#footnote-ref-158)
158. Lete B. Cooperation in cyberspace / B. Lete // NATO Defense College. – 2019. – P. 33–43. [↑](#footnote-ref-159)
159. Zan T. EU-NATO Cyber Cooperation: Who Steps in During a Crisis? / T. Zan // Atlatic Voices. – 2017. № 9(7). – P. 5–11. [↑](#footnote-ref-160)
160. Berelson B. Content-analysis in communication research / B. Berelson. – Glencoe: Free Press, 1952. – 220 p. [↑](#footnote-ref-161)
161. Приложение 5. [↑](#footnote-ref-162)
162. Ахременко А.С. Политический анализ и прогнозирование: введение в количественные методы. Учебное пособие / А.С. Ахременко. – М.: Из-во МГУ, 2012. – С. 25. [↑](#footnote-ref-163)
163. Приложение 6. [↑](#footnote-ref-164)
164. Lete B. EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions // B. Lete, P. Pernik // The German Marshall Fund of the United States. – 2017. № 38. – P. 3–8. [↑](#footnote-ref-165)
165. Cyber Threats and Incident Response Information Sharing Platform (CTIRISP) // PESCO Projects. URL: <https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/> (дата обращения: 13.05.2022). [↑](#footnote-ref-166)
166. Geneva Dialogue for Responsible Behaviour in Cyberspace in the context of international peace and security // Baseline study. 6. 2019. – P. 6–9. URL: <https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Baseline-Study.pdf> (дата обращения: 13.05.2022). [↑](#footnote-ref-167)
167. ENISA official page. URL: <https://www.enisa.europa.eu/about-enisa> (дата обращения 05.05.2022); CSIRTs Network // ENISA. URL: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network?tab=details> (дата обращения: 05.05.2022); ECS official page. URL: <https://ecs-org.eu/> (дата обращения: 05.05.2022); EU ISACs official page. URL: https://www.isacs.eu/ (дата обращения: 05.05.2022); Joint Research Centre // European Commission. URL: <https://ec.europa.eu/info/departments/joint-research-centre_en#related> (дата обращения: 05.05.2022); EC3 // Europol. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения: 05.05.2022). [↑](#footnote-ref-168)
168. NCI Agency official page. URL: <https://www.ncia.nato.int/> (дата обращения: 05.05.2022); Cyber Defence // NATO. URL: <https://www.nato.int/cps/en/natohq/topics_78170.htm> (дата обращения: 05.05.2022); CCD CE official page. URL: <https://ccdcoe.org/> (дата обращения: 05.05.2022); NSO official page. URL: <https://www.natoschool.nato.int/> (дата обращения: 05.05.2022); NDS official page. URL: https://www.ndc.nato.int/ (дата обращения: 05.05.2022); NCI Academy // Agency NCI. URL: <https://www.ncia.nato.int/what-we-do/nci-academy.html> (дата обращения: 05.05.2022). [↑](#footnote-ref-169)