Аналитический отчет

Стратегии кибербезопасности

Оглавление

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch представляет отчет по результатам исследования стратегий государств в отношении кибербезопасности, а также затрагивает вопросы ведения не только оборонительных, но и наступательных операций в киберпространстве.

В данном исследовании мы даём обзор стратегий кибербезопасности ряда государств, а также разбираем, все ли они содержат только оборонительные цели.

Область исследования

Областью исследования стала политика государств в отношении кибербезопасности, отраженная в соответствующих стратегиях различных уровней.

Уровни стратегий

Стратегия кибербезопасности — документ, который фиксирует государственную политику, направленную на обеспечение безопасности государства в киберпространстве.

Для исследования выделены следующие **уровни стратегий кибербезопасности:**

1. Стратегии альянсов государств, как у ЕС и НАТО (у блока НАТО нет официальной стратегии кибербезопасности, но фактически им является «Таллинское руководство по международному праву, применимому к кибервойне», несмотря на то, что оно позиционируется как мнение международной группы экспертов).

2. Государственные (национальные).

3. Отраслевые:

- Мирных отраслей, например, Стратегия гражданской ядерной безопасности Соединенного Королевства.
- По видам вооруженных сил и видам вооружений.

4. Конкретных мероприятий. Например, перед проведением Олимпийских игр 2012 в Лондоне была выпущена отдельная стратегия кибербезопасности данного мероприятия, а в Стратегии кибербезопасности Японии появилась отдельная глава, посвященная безопасности Олимпийских игр 2020 (обзор Стратегии кибербезопасности Японии читайте на нашем сайте).

Выбор государств для анализа их стратегий

В отчете исследованы стратегии кибербезопасности самых активных на мировой арене государств, рассмотрены отдельные подразделения, которые специализируются на проведении не только оборонительных, но и наступательных операций в киберпространстве, разобраны цели создания ведомств, ответственных за кибероперации.

Выбор обусловлен уровнем представленности стран в киберпространстве — это страны, в отношении которых чаще всего упоминаются понятия «кибердержава» или «кибероружие», из них в первую очередь рассмотрены те страны, у которых

документы по исследуемой теме находятся в открытом доступе. Например, несмотря на то, что КНДР часто фигурирует в СМИ, как государство, спонсирующее хакерские группировки и обладающее потенциалом для кибернаступлений, документы в отношении кибербезопасности или кибероперациях этого государства в открытом доступе отсутствуют (в отчете будут приведены выдержки из СМИ).

Определения

Европейское агентство по сетевой и информационной безопасности (ENISA) в 2015 году выпустило документ «Определение кибербезопасности: пробелы и совпадения в стандартизации», где приводит определения понятия «кибербезопасность» в различных международных стандартах и документах.

Организации разных отраслей используют (если используют) свое определение «кибербезопасности».

Например, в СМИ данное понятие употребляется в отношении всего, что может нарушить работу компьютера, и подразумевается «угроза кибербезопасности».

Военные организации или госаппарат подходят к «кибербезопасности» со стратегической точки зрения. Также они **используют понятие «кибербезопасность» в сочетании с термином «кибервойна».**

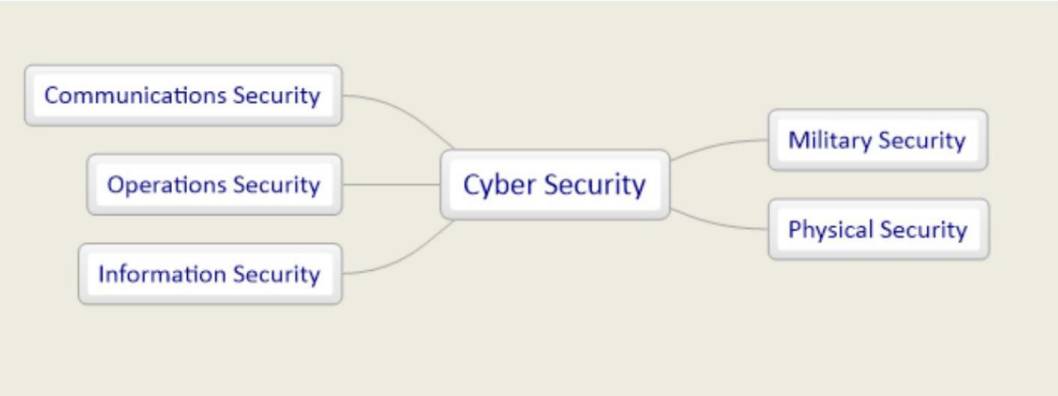

Рисунок 1. Области понятия «кибербезопасность»
(Источник: «Definition of Cybersecurity — Gaps and overlaps in standardisation», The European Union Agency for Network and Information Security (ENISA), 2015)

Области кибербезопасности:

Физическая безопасность — защита от физических угроз, которые могут влиять на состояние киберсистемы. Это физический доступ к серверам, внедрение вредоносного ПО в сеть или принуждение к этому пользователей.

Национальная безопасность — защита от угроз в киберпространстве, которые могут угрожать физическим активам и кибератывам таким образом, что злоумышленник может получить политическую, военную или стратегическую выгоду. Это атаки на системы связи или другую промышленную инфраструктуру.

Безопасность коммуникаций — защита от угроз воздействия на техническую инфраструктуру киберсистем, которое может привести к изменению конфигураций

для выполнения действий, не предусмотренных ее владельцами, разработчиками или пользователями.

Безопасность операций — защита от преднамеренного искажения рабочих процессов, которые могут привести к результатам, не предусмотренным владельцами, разработчиками или пользователями

Информационная безопасность — защита от угрозы кражи, удаления или изменения хранящихся и передаваемых данных в киберсистеме.

Примеры определений

Поскольку в исследовании рассматриваются стратегии зарубежных государств, то в отчете использованы примеры определений из международных стандартов.

Кибербезопасность

Стандарт ISO/IEC 27032:2012[1]

ISO — международная независимая неправительственная организация, в состав которой входят 167 национальных органов по стандартизации.

Кибербезопасность (или безопасность киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве. В свою очередь, киберпространство — это сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологических устройств и подключенных к нему сетей, которые не существуют в какой-либо физической форме.

Стандарт также дает определение **информационной безопасности** — это «сохранение конфиденциальности, целостности и доступности информации».

Международный союз электросвязи[2]

Кибербезопасность — набор инструментов, политик, концепций безопасности, руководств, подходов к управлению рисками, действий, обучения, лучших практик, гарантий и технологий, которые можно использовать для защиты киберсреды, а также активов организации и пользователей.

Активы организации и пользователей включают подключенные вычислительные устройства, персонал, инфраструктуру, приложения, услуги, телекоммуникационные системы и совокупность передаваемой и/или хранимой информации в киберсреде.

Кибербезопасность стремится обеспечить достижение и поддержание свойств безопасности организации и активов пользователя от соответствующих рисков безопасности в киберсреде.

[1] ISO/IEC 27032:2012: https://www.iso.org/
[2] International Telecommunication Union: https://www.itu.int/

NIST National Institute of Standards and Technology[3]

Кибербезопасность — способность защищать и оборонять киберпространство от кибератак.

NATO Cooperative Cyber Defence Centre of Excellence (2012 год)

Не содержит конкретного определения «кибербезопасности», однако указано, что **меры по борьбе с киберугрозами могут носить политический, технологический, юридический, экономический, управленческий или военный характер, а также могут включать другие меры, соответствующие конкретным рискам.**

CNSS - Committee on National Security Systems (Комитет по системам национальной безопасности (США)

Кибербезопасность — предотвращение повреждения, защита и восстановление компьютеров, систем и услуг электронной связи, включая содержащуюся в ней информацию для обеспечения ее доступности, целостности и конфиденциальности.

Кибербезопасность — способность защищать и оборонять использование киберпространства от кибератак.

Все эти определения объединяет тот факт, что, как минимум, в них нет разделения между преднамеренными и непреднамеренными действиями, также в одних определения в качестве угроз идентифицируются только виртуальные ресурсы (например, в стандарте ISO 27000), а в других (например, у НАТО) угроза может носить и виртуальный, и физический характер.

The Chairman of the Joint Chiefs of Staff (CJCS), 2018

В документе CJCS «Cyberspace Operations» приводится определение:

Безопасность киберпространства — действия, предпринимаемые в охраняемом киберпространстве для предупреждения несанкционированного доступа, эксплуатации или повреждения компьютеров, систем электронных коммуникаций и ИТ-систем, включая информационные технологии платформ, а также содержащейся в них информации для обеспечения ее доступности, целостности, аутентификации, конфиденциальности и неотказуемости.

Иногда определение дают и в самих стратегиях кибербезопасности, например, в Стратегии кибербезопасности эмирата Дубай:

Кибербезопасность — внедрение средств управления и контроля для защиты конфиденциальности, целостности и доступности данных для государственного и частного секторов Дубая и отдельных лиц.

Киберпространство

Согласно стандарту ISO/IEC 27032:2012[4], **киберпространство** представляет собой сложную среду, которая возникает в результате взаимодействия людей, программного

[3] NIST National Institute of Standards and Technology: http://csrc.nist.gov/
[4] ISO/IEC 27032:2012: https://www.iso.org/

обеспечения и услуг в Интернете и поддерживается распределенными по всему миру физическими устройствами информационных и коммуникационных технологий (ИКТ) и подключенными сетями.

Министерство обороны США определяет **киберпространство** как глобальную область в информационной среде, состоящей из взаимозависимых сетей ИТ-инфраструктур и данных, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные процессоры и контроллеры.

Японская стратегия кибербезопасности описывает «**киберпространство**» (яп. サイバー空間) как пространство, основой которого является сеть Интернет и которое расширилось благодаря стремительному развитию цифровых технологий и появлению множества независимых участников. Это среда, в которой могут быть созданы такие объекты интеллектуальной собственности, как технологические инновации и новые бизнес-модели, которые, в свою очередь, будут служить основой для устойчивого развития экономического общества.

Информационное пространство — сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию (Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве, 2011 г.).

Киберпространство состоит из сети Интернет, коммуникационных сетей, компьютерных систем, систем автоматического управления, цифровых устройств и приложений, услуг и данных (Стратегия безопасности киберпространства КНР).

Киберустойчивость — обеспечение непрерывности функционирования ИТ-систем и их доступности в киберпространстве (Стратегия кибербезопасности Дубая).

Кибервойна и информационная война

Слово **«кибервойна»** употребляется для обозначения различных понятий. Мнения на этот счет также разные и официальных определений данного слова все еще нет.

Например, Министерство обороны США (DoD) признает угрозу национальной безопасности, которую представляет злонамеренное использование Интернета, но не дает более четкого определения кибервойны.

Бывший советник администрации президента США и специалист по борьбе с терроризмом Ричард Кларк в своей книге «Кибервойна» определил кибервойну как *«действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения»*[5].

[5] «Cyber War», Clarke, Richard A. HarperCollins, 2010.

Как следует из вышесказанного, подобные действия способны нарушить функционирование государственной и гражданской инфраструктуры, могут вывести из строя объекты КИИ, что может привести к ущербу и даже гибели людей.

Информационная война — в отличие от кибервойны, в ходе которой атакуют компьютеры и системы управления, направлена на манипулирование информацией и, как следствие, общественным сознанием, в том числе, мнением лиц, принимающих решения.

Стратегии кибербезопасности

Стратегия кибербезопасности — документ, который фиксирует и определяет государственную политику, направленную на обеспечение безопасности государства в киберпространстве.

В отчете рассмотрены следующие уровни стратегий кибербезопасности:

1. Стратегии альянсов государств, как, например, у НАТО.

2. Государственные (национальные).

3. Отраслевые:

- мирных отраслей,
- по видам вооруженных сил и видам вооружений.

4. Конкретных мероприятий.

В частности, существует **«Руководство по разработке национальной стратегии кибербезопасности»**, выпущенное в 2018 году. Это совместная публикацией Международного союза электросвязи (МСЭ), Всемирного банка, Секретариата Содружества (Comsec), Организации электросвязи Содружества (СТО) и Экспертного центра НАТО по совместной кибероборонe (NATO CCD COE).

Документ является совокупным набором принципов и примеров передового опыта, касающихся разработки, принятия и применения национальных стратегий кибербезопасности.

1. Российская Федерация

Государственный уровень

Концепция кибербезопасности государства в Российской Федерации отсутствует, в 2010 году был выпущен только проект подобной концепции, но итоговый документ так и не был принят.

Приведённые ниже Стратегия национальной безопасности и Доктрина информационной безопасности рассматривают понятие «информационная безопасность» как «*состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз*», где вопросы безопасности информационных технологий, действий в киберпространстве, по сути, являются лишь одним из уровней обеспечения защиты и практически не рассматриваются.

В качестве аналогов стратегии кибербезопасности в Российской Федерации возможно рассматривать:

«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803[6];

и Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ, в том числе Концепцию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, выписка из которой опубликована на сайте Совета безопасности[7]. Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274.

Термин «кибербезопасность» на русском языке приведен в национальном стандарте Российской Федерации ГОСТ Р 56205-2014 (IEC/TS 62443-1-1:2009) СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели:

3.2.36 **кибербезопасность** (**киберзащита**) (**cybersecurity**): действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов.
Примечание: цель при этом — уменьшить персональный риск травмирования или риск угрозы здоровью населения, риск потери доверия общественности или потребителей, разглашения информации о важных объектах, незащищенности бизнес-объектов или несоответствия нормативам. Эти понятия применимы к любой системе в производственном процессе, которая может включать в себя как независимые, так и связанные компоненты. Коммуникация между системами может осуществляться либо с помощью внутренних сообщений, либо через любые пользовательские или машинные интерфейсы, которые обеспечивают аутентификацию, работу, управление или обмен данными с любой из таких систем управления. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности.

[6] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803).

[7] Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274).

1.1 Стратегия национальной безопасности Российской Федерации

Указом Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» была учреждена новая Стратегия национальной безопасности Российской Федерации[8].

Содержание:

I. Общие положения
II. Россия в современном мире: тенденции и возможности
III. Национальные интересы Российской Федерации и стратегические национальные приоритеты
IV. Обеспечение национальной безопасности
- Сбережение народа России и развитие человеческого потенциала
- Оборона страны
- Государственная и общественная безопасность
- Информационная безопасность
- Экономическая безопасность
- Научно-технологическое развитие
- Экологическая безопасность и рациональное природопользование
- Защита традиционных Российских духовно-нравственных ценностей, культуры и исторической памяти
- Стратегическая стабильность и взаимовыгодное международное сотрудничество

V. Организационные основы и механизмы реализации настоящей Стратегии.

В последней редакции Стратегии по сравнению с ее предшественником появился новый пункт **— «Информационная безопасность».**

В документе также отмечено, что ***силовое противоборство стран переходит в новые среды и киберпространство стало новым полем для военных действий***.

«В случае совершения иностранными государствами недружественных действий, представляющих угрозу суверенитету и территориальной целостности Российской Федерации, в том числе связанных с применением ограничительных мер (санкций) политического или экономического характера либо использованием современных информационно-коммуникационных технологий, Российская Федерация считает правомерным принять симметричные и асимметричные меры, необходимые для пресечения таких недружественных действий, а также для предотвращения их повторения в будущем».

1.2 Доктрина информационной безопасности Российской Федерации[9]

Первая редакция Доктрины была утверждена Президентом 9 сентября 2000 года, вторая редакция, действующая, в 2016 году. Приведем несколько цитат из документа:

[8]Указ Президента Российской Федерации от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"
[9] Доктрина информационной безопасности Российской Федерации от 05.12.2016 г.

б) угроза информационной безопасности Российской Федерации (далее - информационная угроза) — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее - информационная безопасность) — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

Национальные интересы в информационной сфере:

а) **обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информаци**и, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) **обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры**, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации**, в мирное время, в период непосредственной угрозы агрессии и в военное время;**

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;

г) **доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации** и ее официальной позиции по социально значимым событиям в стране и мире;

д) **содействие формированию системы международной информационной безопасности,** направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

В соответствии с военной политикой Российской Федерации ***основными направлениями обеспечения информационной безопасности в области обороны страны являются:***

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются — пресечение, противодействие, нейтрализация деятельности, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами, наносящей ущерб национальной безопасности Российской Федерации.

1.3. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803.

Основные направления состоят из четырёх разделов:

I. Общие положения.

II. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления КВО, и ее основные принципы.

III. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления КВО.

IV. Основные механизмы и этапы реализации государственной политики в области обеспечения безопасности автоматизированных систем управления КВО.

Направления разработаны для реализации основных положений Стратегии национальной безопасности Российской Федерации 2020 года, с целью совершенствования безопасности функционирования информационных и телекоммуникационных систем КВО инфраструктуры и объектов повышенной опасности в РФ.

Целью политики является снижение уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

В основных направлениях приведены и используются следующие понятия:

а) критически важный объект инфраструктуры Российской Федерации;
б) автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации (далее - автоматизированная система управления КВО);
в) критическая информационная инфраструктура Российской;
г) компьютерная атака;
д) безопасность автоматизированной системы управления КВО;
е) безопасность критической информационной инфраструктуры;
ж) компьютерный инцидент;
з) единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов;
и) силы обнаружения и предупреждения компьютерных атак;
к) средства обнаружения и предупреждения компьютерных атак;
л) силы ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;
м) средства ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре.

Реализация Основных направлений расписана на 3 этапа — 2014-2020 гг.

Каких-либо отчётов о выполнении мероприятий, указанных в Основных направлениях, а также документов, ссылающихся на него, в открытом доступе найти не удалось, но ***несомненно, что нормативные правовые акты, относящиеся к защите АСУТП КВО (ФСТЭК, 2014 г.), к безопасности критической информационной инфраструктуре Российской Федерации (2017-2022 гг.), соответствуют положениям Основных направлений.***

1.4 «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве»[10], выпущен в 2011 году Минобороны РФ.

[10] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве, 2011 г.

Документ опирается на предыдущую редакцию Доктрины информационной безопасности.

«Наряду с сухопутным, морским, воздушным и космическим пространством, информационное пространство в армиях наиболее развитых стран стало активно использоваться для решения широкого круга военных задач».

Документ состоит из 4 частей:

1. Термины и определения.
2. Принципы.
3. Правила.
4. Меры доверия.

В целом, данный документ посвящен не операциям в киберпространстве, а подчеркивает необходимость противодействия актам информационной войны, включающих психологические операции.

Военный конфликт в информационном пространстве — форма разрешения межгосударственных или внутригосударственных противоречий с применением информационного оружия.

Деятельность вооруженных сил в информационном пространстве — использование вооруженными силами информационных ресурсов для решения задач обороны и безопасности.

Информационное пространство — сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

Информационное оружие — информационные технологии, средства и методы, применяемые в целях ведения информационной войны.

В документе дается и определение информационной войны:

Информационная война — противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Деятельность Вооруженных Сил Российской Федерации в информационном пространстве строится исходя из совокупности принципов: законности, приоритетности, комплексности, взаимодействия, сотрудничества, инновационности.

В условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права.

В целом деятельность в информационном пространстве включает мероприятия штабов и действия войск по разведке, оперативной маскировке, радиоэлектронной борьбе, связи, скрытому и автоматизированному управлению, информационной работе штабов, а также защите своих информационных систем от радиоэлектронных, компьютерных и иных воздействий.

Как итог, даже с учетом определений, весь документ направлен на сдерживание и предотвращение конфликтов, т.е. носит «оборонительный» характер.

2. США

Государственный уровень

2.1 Национальная киберстратегия[11]

«Национальная киберстратегия» США опубликована в сентябре 2018 года и подписана действующим на тот момент президентом Д. Трампом.

Министерства обороны США:

«Мы ведем долгосрочную стратегическую конкуренцию с Китаем и Россией. Эти государства усилили эту конкуренцию, включив в нее постоянные кампании в киберпространстве, которые представляют стратегический риск в долгосрочной перспективе для нации, а также для наших союзников и партнеров. Китай подрывает военное превосходство США и экономическую жизнеспособность страны, настойчиво извлекая конфиденциальную информацию из государственных и частных учреждений США. Россия использовала информационные операции с применением кибертехнологий, чтобы повлиять на наше население и бросить вызов нашим демократическим процессам. Другие субъекты, такие как Северная Корея и Иран, аналогичным образом использовали злонамеренные действия в киберпространстве, чтобы нанести ущерб гражданам США и угрожать интересам США. Масштабы и темпы злонамеренной кибератаки продолжают расти. Растущая зависимость Соединенных Штатов от киберпространства почти для всех основных гражданских и военных функций делает это неприемлемым риском для нации».

«Министерство обороны США должно принимать меры в киберпространстве, чтобы сохранить военное преимущество США и защитить интересы США. Наше внимание будет сосредоточено на государствах, которые представляют стратегическую угрозу процветанию и безопасности США, особенно на Китае и России. Мы будем проводить операции в киберпространстве для сбора разведывательных данных и подготовки военных кибервозможностей для использования в случае кризиса или конфликта. Мы будем защищаться, чтобы прервать или остановить злонамеренную кибератаку в корне, включая деятельность, которая не

[11] National Cyber Strategy of the United States of America, 2018.

соответствует уровню вооруженного конфликта. Мы укрепим безопасность и устойчивость сетей и систем, которые способствуют текущим и будущим военным преимуществам США. Мы будем сотрудничать с нашими межведомственными, отраслевыми и международными партнерами для продвижения наших общих интересов».

«В военное время киберсилы США будут готовы действовать вместе с нашими воздушными, наземными, морскими и космическими силами, чтобы наносить удары по слабым местам противника, нивелировать сильные стороны противника и повышать эффективность других элементов объединенных сил. Вооруженные силы противника все больше полагаются на тот же тип компьютерных и сетевых технологий, которые стали ключевыми в боевых действиях объединенных сил. Министерство обороны будет использовать эту зависимость для получения военного преимущества. Объединенные силы будут использовать наступательные кибервозможности и инновационные концепции, которые позволят использовать операции в киберпространстве во всем спектре конфликтов».

Киберстратегия состоит из четырех частей:

1. «Защита американского народа, родины и американского образа жизни», в которой говорится о безопасности федеральных сетей, критической информационной инфраструктуры, о борьбе с киберпреступностью и улучшении отчетности о киберинцидентах.

2. «Содействие процветанию Америки». В этой части говорится о цифровой экономике, содействию развитию безопасного рынка технологий, о сохранении США как лидера в создании новых технологий.

3. **«Сохранение мира силой»**, которая содержит меры противодействия «неприемлемому» поведению в киберпространстве. Именно в этой части говорится о действиях в киберпространстве.

4. «Усиление американского влияния», говорит о сохранении безопасного и свободного Интернета, а также об усилении киберпотенциала страны.

В стратегии США чаще вместо употребления слова **«киберпространство»** в основном, делают **акцент на сети Интернет**. Цитата: «***Америка создала Интернет и поделилась им со всем миром. Теперь мы должны убедиться в безопасности киберпространства для будущих поколений***». Что примечательно, определения «киберпространство» в американской стратегии не дается.

Целью 3 части Стратегии определено следующее:

«Выявление, противодействие, разрушение и сдерживание поведения в киберпространстве, которое дестабилизирует и противоречит национальным интересам США, сохраняя при этом превосходство Соединенных Штатов в киберпространстве».

В список мер против действий, наносящих ущерб США, входят «все инструменты национальной власти». Это «дипломатические, информационные, военные (кинетические и кибернетические), разведывательные и финансовые возможности».

В главе также указано, что разведывательное сообщество (Intelligence Community, IC) будет и впредь лидировать в использовании кибервразведки из всех источников для выявления и установления источника злонамеренной киберактивности, которая угрожает национальным интересам Соединенных Штатов.

Соединенные Штаты будут использовать все соответствующие инструменты национальной власти для разоблачения и противодействия потоку злонамеренного влияния в Интернете и информационных кампаний, а также негосударственной пропаганды и дезинформации. Это включает в себя работу с иностранными государственными партнерами, а также с частным сектором, академическими кругами и гражданским обществом для выявления, противодействия и предотвращения использование цифровых платформ для злонамеренных операций иностранного влияния при соблюдении гражданских прав и свобод.

В общем и целом, Киберстратегия США носит агрессивный характер, заявляет о мировом господстве США в киберпространстве, а также оправдывает любые действия правом сильного.

Отраслевые стратегии

2.3 Cyberspace Operations[12] (2018)

«Операции в киберпространстве» — это доктрина для планирования, выполнения и оценки операций в киберпространстве.

Предыдущая редакция документа была выпущена в 2013 году и носила закрытый характер, но в 2018 году документ стал открытым. В нем Киберкомандование США позиционируется как функциональное боевое командование.

В документе излагается доктрина, регулирующая действия вооруженных сил Соединенных Штатов в совместных операциях[13], а также рассматриваются вопросы военного взаимодействия с правительственными и неправительственными учреждениями, многонациональными силами и другими партнерами. Он обеспечивает военное руководство по осуществлению полномочий комбатантами и другими командующими объединенными силами (JFC), а также предписывает совместную доктрину для операций и обучения.

В отличие от Киберстратегии, в данном документе есть определение безопасности киберпространства, см. раздел «Определения».

Т.е. кибербезопасность определяется как действия, предпринимаемые для предотвращения несанкционированного доступа, эксплуатации или повреждения компьютеров, систем электронных коммуникационных систем и других информационных технологий, включая содержащуюся в системах информацию.

[12] Cyberspace Operations, the Chairman of the Joint Chiefs of Staff (CJCS), 2018.
[13] Joint Force's Use of Cyberspace, в документе — JFC.

2.4 Strategic principles for securing the Internet of Things[14] (IoT)

Документ выпущен Министерством внутренней безопасности США в 2016 году.

В этом документе объясняются риски для безопасности и экономики и приводится набор необязательных принципов и рекомендуемых передовых методов для обеспечения ответственного уровня безопасности устройств и систем Интернета вещей, которые разрабатываются и эксплуатируются предприятиями.

2.5 Концепция по улучшению безопасности критической инфраструктуры[15] (2014)

Президент США издал Указ № 13636 «Повышение кибербезопасности критически важной инфраструктуры» от 12 февраля 2013 г., в котором было установлено, что «Политика Соединенных Штатов направлена на повышение безопасности и устойчивости национальной инфраструктуры».

Указ призывает к разработке добровольной концепции кибербезопасности — набора отраслевых стандартов и передовых методов, помогающих организациям управлять рисками кибербезопасности. Получившаяся в результате платформа, созданная в результате сотрудничества между правительством и частным сектором, действует слаженно для устранения и управления рисками кибербезопасности экономически эффективным способом, основанным на потребностях бизнеса, без дополнительных нормативных требований к бизнесу.

3. НАТО

Стратегия альянса государств

3.1 Таллинское руководство по международному праву, применимому к кибервойне[16] (2013)

Данное Руководство, несмотря на распространённое заблуждение, не является официальным документом, а лишь мнением Международной группы экспертов в области права, приглашенных Центром передового опыта совместной кибербезопасности НАТО.

«Цель проекта никогда не состояла в том, чтобы принять закон или создать руководство, имеющее силу закона».

Первую редакцию готовили эксперты по праву вооруженных конфликтов преимущественно из западных стран, что вызвало критику. И для подготовки 2-ой редакции документа группа экспертов стала шире по географическому принципу и уже включала в себя представителей Японии, Таиланда, Китая, а также в нее вошли эксперты в области прав человека, космического права и международного телекоммуникационного права.

На данный момент действует 2 редакция документа, выпущенная в 2013 году.

[14] Strategic principles for securing the Internet of Things, U.S. Department of Homeland Security, 2016
[15] Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2014
[16] The Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013.

После начала событий 24 февраля 2022 года, в СМИ появились сообщения о подготовке 3 редакции Руководства, в которой собираются обозначить Россию как непосредственную угрозу Альянсу.

Руководство состоит почти из 150 правил, ниже приведены выдержки:

- Руководство начинается с понятий о суверенитете и подчеркивает, что «принцип суверенитета применим и к киберпространству» и какое-либо государство не должно проводить кибероперации, нарушающие суверенитет другого государства.
- Государства не должны допускать, чтобы их территория или киберинфраструктура, находящаяся под государственным контролем, использовались для атак на другие государства. Государства ответственны за кибероперации против других государств, которые ведутся с их территории, даже если такие операции ведутся не спецслужбами.
- Кибероперации, проводимые в рамках вооруженного конфликта, попадают под действие права вооруженных конфликтов. Кибероперации, которые привели к жертвам среди гражданского населения, расцениваются как военные преступления. И одновременно говорится, что нанесение физического ущерба или телесных повреждений не является обязательными условиями для того, чтобы кибероперация считалась противоправной.
- Государство вправе принять соразмерные контрмеры в ответ на нападение. При этом считается незаконным принятие контрмер непострадавшим государством от имени пострадавшего.
- Государство, ставшее жертвой нападения в киберпространстве, повлекшего человеческие жертвы или иной ущерб, имеет право ответить с помощью военной силы в физическом мире.
- Запрещено использовать кибероперации для того, чтобы сеять страх среди населения.

4. Соединенное Королевство

Государственный уровень

4.1 Национальная стратегия кибербезопасности[17] (2022)

Содержание:

Часть 1: Стратегия.
Часть 2: Реализация.
- 2.1: Киберэкосистема Соединенного Королевства.
- 2.2: Киберустойчивость.
- 2.3: Технологическое преимущество.
- 2.4: Глобальное лидерство.
- 2.5: Противодействие угрозам.

Приложения.

[17] National Cyber Security Strategy 2022: https://www.gov.uk

Главная **цель** данной Стратегии кибербезопасности — к 2025 году повысить устойчивость важнейших функций правительства Соединенного Королевства к кибератакам, при этом все организации в государственном секторе должны быть устойчивы к известным уязвимостям и методам атак не позднее 2030 года.

«Стратегия сконцентрирована вокруг двух основных направлений, первое из которых сосредоточено на создании прочной основы организационной устойчивости к кибербезопасности; а второе направлено на то, чтобы позволить правительству «защищаться как единое целое», используя ценность обмена данными, опытом и возможностями», сказал в интервью Винсент Дивайн, глава службы безопасности правительства.

*«Мы вложили значительные средства в наши наступательные кибервозможности через **Национальную наступательную киберпрограмму** (National Offensive Cyber Programme), а теперь и в новые **Национальные киберсилы (NCF)**. Мы также разработали комплексный ответ национальных правоохранительных органов под руководством Национального агентства по борьбе с преступностью (NCA) и стремились разрушить, а также повысить стоимость враждебной и преступной деятельности в киберпространстве».*

Национальные киберсилы

В части 2.5 Киберстратегии упоминаются **Национальные киберсилы (NCF),** созданные в 2020 году, отвечают за проведение операций в киберпространстве с целью противостояния, разрушения и борьбы с теми, кто может причинить вред Великобритании или ее союзникам, обеспечивать безопасность страны, а также защищать и продвигать интересы Великобритании внутри страны и за рубежом. NCF состоит из примерно равного соотношения сотрудников из структур обороны и разведки.

NCF нацелены на достижение результатов в интересах национальной безопасности, таких как поддержка обороны, экономическая стабильность Соединенного Королевства и предупреждение действий в киберпространстве против как государственных, так и негосударственных субъектов.

Работа Национальных киберсил делится на три основные категории:

1. Противодействие угрозам со стороны террористов, преступников и государств, использующих Интернет для трансграничных операций с целью причинения вреда Великобритании и другим демократическим обществам.
2. Противодействие угрозам, которые нарушают конфиденциальность, целостность и доступность данных и услуг в киберпространстве (**т.е. обеспечение кибербезопасности**).
3. Участие в операциях обороны Соединенного Королевства и помощь в реализации внешнеполитической программы.

   Операции NCF могут быть проведены для воздействия на отдельных лиц и группы, нарушения работы онлайн-систем и систем связи, а также для ухудшения работы

физических систем. Этот вид деятельности часто называют наступательной кибербезопасностью.

Операции NCF проводятся в соответствии с правовой базой Соединенного Королевства, которая включает Закон о разведывательных службах 1994 года и Закон о полномочиях по расследованию 2016 года.

Виды оперативной деятельности, которые может проводить NCF, включают:

- Препятствование осуществлению террористическими группами своих планов путем отключения их командно-административной связи и ограничения распространения экстремистских СМИ.
- Снижение риска причинения вреда вооруженным силам Соединенного Королевства за счет деградации систем вооружения противника.
- Защита демократии и свободных, справедливых и открытых выборов путем противодействия организованным государством кампаниям по дезинформации, направленным на их подрыв
- Предотвращение получения преступными группами прибыли от их деятельности путем нарушения использования ими онлайн-платформ и услуг.
- Помощь в обеспечении соблюдения международных санкций путем срыва усилий по их обходу.
- Защита Соединенного Королевства и других стран от кибератак путем нарушения работоспособности инфраструктуры, используемой злоумышленниками для их осуществления.
- Защита гражданских лиц в условиях гуманитарного кризиса путем сохранения для них возможности доступа к критически важной информации.

Отраслевой уровень

4.2 Government Cyber Security Strategy 2022-2030

Цель стратегии: создание киберустойчивого государственного сектора.

4.3 Civil Nuclear Cyber Security Strategy[18] (2022)

В документе изложены четыре ключевые задачи, которые необходимо выполнить до 2026 года:

1. Приоритизация кибербезопасности как части целостного подхода к управлению рисками и регулирования, ориентированного на результат.
2. Упреждающее снижение киберрисков в отрасли и по всей цепочке поставок на фоне устаревших и новых технологий.
3. Повышенная отказоустойчивость за счет лучшей подготовки к инцидентам и реагирования на них быстрее и в большей степени совместными усилиями, сводя к минимуму последствия и время восстановления.

[18] Civil Nuclear Cyber Security Strategy, 2022.

4. Больше сотрудничества для повышения киберзрелости, развития навыков и продвижения культуры, ориентированной на безопасность.

Стратегии безопасности мероприятий

4.4 Olympic and Paralympic Safety and Security Strategy[19] (2011)

Стратегия, выпущенная к Олимпийским и Паралимпийским играм в Лондоне 2012.

5. Канада

Государственный уровень

5.1 Национальная стратегия кибербезопасности (2018)[20]

Стратегия кибербезопасности Канады выпущена с акцентом на потенциал растущего лидерства Канады в этой области. Стратегия основана более чем на 2000 материалах, направлена на устранение пробелов и развитие областей, требующих улучшения в области кибербезопасности.

В Стратегии также отмечены значительные инвестиции в кибербезопасность, на общую сумму более 500 миллионов долларов США в течение 5 лет. Бюджет на 2018 год является крупнейшей разовой инвестицией в кибербезопасность, когда-либо сделанной правительством Канады.

Содержание:

Резюме

- Место Канады в цифровом мире
- Важность кибербезопасности
- Видение национальной стратегии кибербезопасности: безопасность и процветание в эпоху цифровых технологий
- Объем стратегии
- Реализация стратегии

Введение

- Основа на достижениях Канады в динамичном киберпространстве

Безопасность и устойчивость

- Стратегический контекст: эволюция киберугроз
- Киберпреступность и сложные киберугрозы
- Растущее влияние
- Публичные консультации по кибербезопасности
- Безопасные и отказоустойчивые канадские системы

Киберинновации

- Стратегический контекст: расширение границ кибербезопасности
- Новые горизонты технологий и развития бизнеса
- Использование преимуществ цифровых технологий
- Развитие навыков и знаний 21 века

[19] Olympic and Paralympic Safety and Security Strategy, 2011.
[20] National Cyber Security Strategy, 2018.

- Публичные консультации по кибербезопасности
- Инновационная и адаптивная кибер-экосистема

Лидерство и сотрудничество

- Стратегический контекст: сотрудничество для реализации преимуществ цифровой жизни
- Повышение базовой кибербезопасности в Канаде
- Федеральное лидерство в области кибербезопасности в динамичной среде
- Публичные консультации по кибербезопасности
- Эффективное лидерство, управление и сотрудничество

В стратегии **определение кибербезопасности** приводится как *«защита цифровой информации, а также целостность инфраструктуры размещения и передачи цифровой информации. В частности,* ***кибербезопасность включает совокупность технологий, процессов, методов, а также мер реагирования и смягчения последствий, предназначенных для защиты сетей, компьютеров, программ и данных от атак, повреждений или несанкционированного доступа с целью обеспечения конфиденциальности, целостности и доступности****»*.

Стратегии безопасности мероприятий

Стратегия безопасности Олимпийских игр в Ванкувере, 2010 год.

6. Австралия

Государственный уровень

6.1 Стратегия кибербезопасности[21]

Австралийская стратегия кибербезопасности 2020 года предусматривает инвестиции в размере 1,67 миллиарда долларов в течение 10 лет для реализации создания более безопасного онлайн-мира для австралийцев, бизнеса и услуг.

Стратегия реализуется с помощью действий:

- правительства по усилению защиты австралийцев, предприятий и критической инфраструктуры от угроз и др.;
- предприятий по обеспечению безопасности своих продуктов и услуг и защите своих клиентов от известных киберуязвимостей;
- сообщества по безопасному поведению в Интернете и принятию обоснованных решений о покупках.

[21] Australia's Cyber Security Strategy, 2020.

7. Япония

Государственный уровень

7.1 Стратегия кибербезопасности

Последняя редакция стратегии опубликована в 2018 году, в ней определены цели и меры их достижения в сфере кибербезопасности на среднесрочный период 2018-2021 годы внутри страны и за ее пределами, а также появилась глава, посвященная обеспечению кибербезопасности при проведении Олимпийских и Паралимпийских игр в 2020.

Помимо обеспечения безопасности Олимпийских игр, в Стратегии особое внимание уделено кибербезопасности объектов КИИ.

Японская стратегия кибербезопасности состоит из **пяти разделов:**

1. Введение, в котором говорится о смене социальной парадигмы из-за слияния физического и киберпространства, и описываются произошедшие изменения с 2015 года.
2. Понятие киберпространства и увеличение количества киберугроз.
3. Цели и задачи стратегии.
4. Меры для достижения целей.
5. Внедрение и продвижение кибербезопасности.

Цели стратегии:

1. улучшение социально-экономических условий и устойчивое развитие;
2. создание для людей безопасного и мирного общества;
3. внесение вклада в мир и устойчивость международного сообщества и национальной безопасности.

Общую цель Стратегия описывает как **развитие киберпространства в качестве «рубежа для создания бесконечных ценностей», которые приносят людям изобилие и процветание.**

Подробнее стратегию кибербезопасности Японии мы рассмотрели в отдельном обзоре, опубликованном на нашем сайте[22].

Стратегия кибербезопасности Японии пересматривается раз в три года, последняя редакция выпущена в 2018 году, в анонсе новой Стратегии 2021 года Китай и Россия позиционируются как соперники, в частности, пишется об ухудшении отношений с Россией.

[22] «Япония: обзор стратегии кибербезопасности»: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/yaponiya-obzor-strategii-kiberbezopasnosti

8. КНР

Государственный уровень

8.1 Национальная стратегия безопасности киберпространства[23] (2016)

Стратегия излагает основные позиции и предложения Китая в отношении развития и безопасности киберпространства и служит руководством для работы Китая в области кибербезопасности. ***Стратегия направлена на то, чтобы превратить Китай в кибердержаву***, продвигать упорядоченное, безопасное и открытое киберпространство и защищать национальный суверенитет. Стратегия рассматривает кибербезопасность как «новую территорию национального суверенитета» и знаменует собой новый шаг в рационализации киберконтроля.

К основным задачам Стратегии относятся:

1. Защита суверенитета киберпространства.
2. Защита национальной безопасности.
3. Защита критической информационной инфраструктуры (CII).
4. Создание здоровой онлайн-культуры.
5. Борьба с киберпреступностью, шпионажем и терроризмом
6. Совершенствование киберуправления.
7. Повышение базовой кибербезопасности.
8. Повышение возможностей защиты киберпространства.
9. Укрепление международного сотрудничества.

Стратегия определяет сферу КИИ как включающую сети связи и радиовещания, энергетику, финансы, транспорт, образование, научные исследования, гидравлические системы, промышленное производство, здравоохранение, социальное обеспечение, государственные услуги, а также информацию и интернет-приложения, системы для государственных учреждений.

8.2 International Strategy of Cooperation on Cyberspace (2017)[24]

Из предисловия Стратегии:

«Киберпространство является общим пространством деятельности человечества. Будущее киберпространства должно быть в руках всех стран. Странам следует активизировать общение, расширять консенсус и углублять сотрудничество для совместного создания сообщества общего будущего в киберпространстве» (Си Цзиньпин).

Что примечательно, в отличие от стратегии США, в «Международной стратегии сотрудничества в киберпространстве» Китая сеть **Интернет** позиционируется как **«общее достояние человеческого общества».**

[23] Национальная стратегия безопасности киберпространства, КНР, 2016.
[24] International Strategy of Cooperation on Cyberspace. Ministry of Foreign Affairs of the People's Republic of China, The Department of Arms Control.

Данная стратегия сотрудничества в киберпространстве объясняет политику и позицию Китая в международных вопросах, связанных с киберпространством, а также основные принципы, стратегические цели и план действий во внешних отношениях на этом фронте. Документ призван показать участие Китая в международном обмене и сотрудничестве в киберпространстве в течение следующего периода времени и призвать международное сообщество объединиться для диалога и сотрудничества, а также построения мирного, безопасного, открытого, кооперативного и упорядоченного киберпространства и многосторонней, демократической и прозрачной глобальной системы управления Интернетом.

Содержание Стратегии:

Китай наравне с Россией в большей степени затрагивает вопрос защиты собственного суверенитета в киберпространстве (цитата из главы «Защита суверенитета и безопасности»):

«Китай решительно выступает против того, чтобы любая страна использовала Интернет для вмешательства во внутренние дела других стран, и считает, что каждая страна имеет право и обязанность поддерживать свою кибербезопасность и защищать законные права и интересы различных сторон в киберпространстве с помощью национальных законов и политик. Тенденция милитаризации и

наращивания сдерживания в киберпространстве не способствует международной безопасности и стратегическому взаимному доверию. Китай призывает все стороны к мирному урегулированию споров».

Национальная стратегия безопасности (2015)

В открытом доступе не найдена.

8.3 National Military Strategy[25] (2014)

Данная стратегия не относится к киберстратегиям, однако в ней также уделено внимание киберпространству.

«Мировая революция в военном деле (ВВР) переходит на новый этап. Все более совершенными становятся дальнобойные, точные, умные, малозаметные и беспилотные вооружения и техника. Космическое пространство и ***киберпространство*** *стали новыми командными высотами в стратегическом соревновании между всеми сторонами. Форма войны ускоряет свою эволюцию информатизации. Крупнейшие мировые державы активно корректируют свои стратегии национальной безопасности и оборонную политику, а также ускоряют свою военную трансформацию и реструктуризацию вооруженных сил. Вышеупомянутые революционные изменения в военных технологиях и формах войны не только оказали значительное влияние на международную политическую и военную ситуацию, но и поставили перед военной безопасностью Китая новые серьезные вызовы».*

Не представлены в Стратегиях, но существуют органы КНР по кибербезопасности, это:

- Управление киберпространства Китая (CAC) — центральный орган регулирования интернета, цензурный, надзорный и контролирующий орган Китайской Народной Республики.
- Национальный технический комитет по стандартизации информационной безопасности («TC260»).
- Национальный центр кибербезопасности Китая (NCC), о создании котором было объявлено недавно, в 2021 году.

9. Украина

Государственный уровень

Стратегия кибербезопасности

Указом Президента Украины от 26 августа 2021 г. № 447/2021 была утверждена новая Стратегия кибербезопасности, которая ранее (еще в мае 2021 года) была одобрена Советом национальной безопасности и обороны Украины.

Содержание:

1. Кибербезопасность: глобальный контекст.

[25] China's Military Strategy, 2014.

2. Состояние реализации Стратегии кибербезопасности Украины, утвержденной Указом Президента Украины от 15 марта 2016 г. № 96.
3. Национальное киберпространство: вызовы и киберугрозы.
4. Национальная система кибербезопасности: основы развития.
5. Приоритеты обеспечения кибербезопасности и стратегические цели.
6. Стратегические задачи.
7. Направления внешнеполитической деятельности Украины в сфере кибербезопасности.
8. Механизмы реализации стратегии и обеспечения открытости.
9. Измерения успеха (метрики).

Далее приведены некоторые из цитат.

«1. Кибербезопасность: глобальный контекст

Удельный вес киберугроз растет, и эта тенденция по мере развития информационных технологий и их конвергенции с технологиями искусственного интеллекта в ближайшее десятилетие будет усиливаться. Рост такого влияния на функционирование структур управления как национальных, так и транснациональных формирует новую ситуацию безопасности. Между мировыми центрами силы происходит разделение сфер влияния в киберпространстве, усиливается их стремление за счет такого разделения обеспечить реализацию собственных геополитических интересов.

***Киберпространство вместе с другими физическими пространствами признано одним из возможных театров военных действий**. Набирает силу тенденция по созданию кибервойск, в задачи которых входит не только обеспечение защиты критической информационной инфраструктуры от кибератак, но и проведение превентивных наступательных операций в киберпространстве, включающий вывода из строя критически важных объектов инфраструктуры противника путем разрушения информационных систем, которые управляют такими объектами».*

*В Стратегии утверждается, что «**Российская Федерация остается одним из основных источников угроз национальной и международной кибербезопасности**, активно реализует концепцию информационного противоборства, основанную на сочетании деструктивных действий в киберпространстве и информационно-психологических операций, механизмы которой активно применяются в гибридной войне против Украины. Такая деструктивная активность создает реальную угрозу совершения актов кибертерроризма и кибердиверсий относительно национальной информационной инфраструктуры», - отмечается в стратегии».*

Среди вызовов для Украины в сфере кибербезопасности указаны:

«Милитаризация киберпространства и развитие кибероружия, что позволяет скрыто проводить кибератаки для поддержки боевых действий и разведывательно-подрывной деятельности в киберпространстве».

Первым пунктом в списке угроз кибербезопасности Украины является:

«Гибридная агрессия Российской Федерации против Украины в киберпространстве Государство-агрессор постоянно наращивает арсенал кибероружия наступательного назначения, применение которого может вызвать неисправимые, необратимые разрушительные последствия. Кибератаки Российской Федерации направлены прежде всего на информационно-коммуникационные системы государственных органов Украины и объекты критической информационной инфраструктуры с целью выведения их из строя (кибердиверсия), получения скрытого доступа и контроля, осуществления разведывательной и разведывательно-подрывной деятельности. Кибератаки также активно используются государством-агрессором как элемент специальных информационных операций с целью манипулятивного влияния на население, вмешательства в избирательные процессы и дискредитации украинской государственности».

Стратегия кибербезопасности, на первый взгляд, позиционируется на основе сдерживания угроз.

В Стратегии указывается, что «для формирования потенциала сдерживания необходимо достижение следующих стратегических целей:

«***цель С.1.*** *Действенная кибероборона — Украина создаст и обеспечит развитие (в том числе кадрово и технологически) подразделений с полномочиями ведения вооруженного противоборства в киберпространстве, сформирует надлежащую правовую, организационную, технологическую модель их функционирования и применения, обеспечит эффективное взаимодействие основных субъектов национальной системы кибербезопасности обороны при проведении мероприятий по кибероборонe, надлежащее обучение и финансовое обеспечение таких структур, систематическое проведение киберучений, оценку возможностей и эффективности подразделений, разработку и имплементацию индикаторов оценки их деятельности;*

цель С.2. *Эффективное противодействие разведывательно-подрывной деятельности в киберпространстве и кибертерроризме — Украина обеспечит непрерывное осуществление контрразведывательных мероприятий по выявлению, предупреждению и пресечению разведывательно-подрывной деятельности иностранных государств, актов кибершпионажа и кибертерроризма, устранению условий, которые им способствуют, общества и отдельных граждан;*

цель С.3. *Эффективное противодействие киберпреступности — Украина обеспечит приобретение правоохранительными органами и государственным органом специального назначения с правоохранительными функциями способностей для минимизации угроз киберпреступности, усиления их технологического и кадрового потенциала для проведения превентивных мероприятий и расследования киберпреступлений;*

цель С.4. *Развитие асимметричных инструментов сдерживания Украина создаст необходимые условия для обеспечения сдерживания агрессивных действий в киберпространстве против Украины путем применения экономических, дипломатических, разведывательных мероприятий, а также привлечения потенциала частного сектора».*

При этом заявлено и о создании кибервойск:

«Для достижения цели С.1 Украина сформирует систему действенной кибероборонs путем:

образования в системе Министерства обороны Украины ***кибервойск*** *и обеспечение их надлежащими финансовыми, кадровыми и техническими ресурсами для сдерживания вооруженной агрессии в киберпространстве и предоставления отпора агрессору;*

проведение не менее двух раз в год ***совместных тематических учений с соответствующими подразделениями государств-членов НАТО*** *для достижения оперативной совместимости».*

Итого мы видим, что Стратегия Украины носит агрессивный и антироссийский характер.

10. Дубай

Государственный уровень

Dubai Cyber Security Strategy[26]

Данный документ примечателен тем, что это стратегия не государства Объединенные Арабские Эмираты, а эмирата Дубай.

Цель стратегии: сделать Дубай мировым лидером в области инноваций и кибербезопасности, а также заявлена цель по созданию «Cyber Smart Society».

Согласно документу, «***стратегия является частью усилий в стремлении сделать ОАЭ самой безопасной в цифровом плане страной мира»***.

Стратегия кибербезопасности Дубая устанавливает правила защиты данных и электронных услуг от угроз и атак, а также защищает компании, отдельных пользователей и любую деятельность, связанную с информационными технологиями.

«Киберпространство взаимосвязано в нескольких измерениях и не может ограничиваться только государственным сектором Дубая или управляться только одной страной или городом. Государственный сектор Дубая должен работать рука об руку с частным сектором. Все заинтересованные стороны в киберпространстве, включая критическую информационную инфраструктуру (CII), должны разделять общее видение кибербезопасности и выполнять свои обязанности в отношении кибербезопасности и киберустойчивости».

В стратегии даются определения кибербезопасности и киберустойчивости (см. раздел Определения).

[26] Dubai Cyber Security Strategy, Dubai Electronic Security Center, 2017.

Активные действия в киберпространстве и подразделения по наступательным операциям

Несмотря на мирный характер большинства заявлений и инициативы по сотрудничеству для противодействия киберпреступности, множество государств уже имеют специальные подразделения для операций в киберпространстве, даже если их Стратегии кибербезопасности не предусматривают применение наступательных операций, также множество официальных лиц неоднократно, прямо или косвенно указывали о проведении кибератак.

Разберемся, как на деле трактуют действия в киберпространстве некоторые государства и какие заявления они делают.

Политика в киберпространстве

Обращение Международного комитета Красного креста

После выпуска второй редакции (2013 г.) «Таллинского руководства» Международный комитет Красного креста (МККК) выпустил бюллетень «**Кибервойна и международное гуманитарное право: позиция МККК»**, в котором выразил обеспокоенность, что у кибервойны нет ограничений и правил, подобных правилам по ведению боевых действий.

При разработке «Таллинского руководства» МККК принял участие в качестве наблюдателя.

Термином **«кибервойна»** МККК определяет ***средства и методы ведения войны, состоящих из кибероперaций, равнозначных вооруженному конфликту или проводимых в контексте вооруженного конфликта***. Также МККК пишет о том, что кибероперации могут иметь разрушительные гуманитарные последствия для гражданского населения, поэтому к таким операциям необходимо применять Международное гуманитарное право.

Нормы поведения в киберпространстве

В декабре 2021 года Генассамблея ООН без голосования приняла совместную резолюцию России и США о нормах поведения в киберпространстве. Название документа: «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий». Россия и США призвали не допускать применения информационных ресурсов или технологий «в преступных или террористических целях».

Среди соавторов: Австралия, Соединённое Королевство, Франция, Германия и др. Также Россия и США пригласили все страны присоединиться к этим правилам поведения в киберпространстве.

Подробнее перечень как мирных инициатив, так и одновременно с ними деклараций о праве на нападение в киберпространстве, проведения ряда операций за последние

12 месяцев читайте в статье главного редактора Ассоциации по защите деловой информации от 10 июня 2022 года.[27]

Женевская и Гаагские конвенции о поведении в киберпространстве

В 2011 году эксперты по кибербезопасности из России и США выпустили совместный отчет о правилах поведения в киберпространстве[28]. Авторы отчета дают пять рекомендаций, выполнение которых поможет сохранить гуманитарные принципы ведения войны. Авторы также дают свою интерпретацию Женевской и Гаагской конвенций о киберпространстве.

США

Создание Киберкомандования США

Операциями в киберпространстве управляет одно из подразделений Министерства обороны США — **Киберкомандование США (USCYBERCOM[29]).** Подразделение было создано в 2009 году в штаб-квартире Агентства национальной безопасности (АНБ). Помимо того, что Киберкомандование сотрудничает с АНБ, его по совместительству возглавляет директор Агентства национальной безопасности США. В 2017 году подразделение повысили и присвоили ему статус полноценного и независимого боевого командования[30].

В течение периода существования данного подразделения неоднократно поднимался вопрос о разделении и отказе от совместного руководства Агентством национальной безопасности и Киберкомандованием США, поскольку шпионажем и кибервойной должны заниматься разные структуры[31]. В 2016 году за разделение выступал и министр обороны США Эштон Б. Картер, намереваясь превратить Киберкомандование в полноценную боевую силу для проведения кибератак.

Официальная миссия Киберкомандования в текущей редакции носит оборонительный характер:

«Направлять, синхронизировать и координировать планирование и операции в киберпространстве — для защиты и продвижения национальных интересов — в сотрудничестве с местными и международными партнерами».

Однако несколько лет назад при другом командующем миссия звучала так:

*«USCYBERCOM планирует, координирует, интегрирует, синхронизирует и проводит мероприятия по: управлению операциями и защите определенных информационных сетей Министерства обороны; готовится и по указанию **проводит полномасштабные военные операции в киберпространстве**, чтобы обеспечить*

[27] «Кибербезопасность, киберпреступность и кибервойны. Прошёл год»: https://bisa.ru/glavred-bdit/kiberbezopasnost-kiberprestupnost-i-kibervoyny-proshyol-god
[28] «Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace, Russia-U.S. bilateral on critical infrastructure protection», 2011.
[29] U.S. Cyber Command: https://www.cybercom.mil/
[30] «Statement by President Donald J. Trump on the Elevation of Cyber Command», 2017: https://trumpwhitehouse.archives.gov/
[31] «The Washington Post. Obama to be urged to split cyberwar command from NSA», The Washington Post, 2016.

возможность действий во всех областях, обеспечить свободу действий США и союзников в киберпространстве и лишить того же наших противников».

В СМИ и заявлениях политиков деятельность Киберкомандования США фигурирует как сила для ведения кибервойн.

В мае 2022 года Госдепартамент США выпустил официальный информационный бюллетень «Поддержка США для связи и кибербезопасности Украины», в котором перечислил, какую помощь оказывает Украине[32]. В том числе:

- Федеральное бюро расследований (ФБР) оказывало непосредственную поддержку своим украинским партнерам по национальной безопасности и правоохранительным органам, включая информирование украинских партнеров о кибероперациях российских спецслужб.
- Технические эксперты, финансируемые Агентством США по международному развитию (USAID), оказывают практическую поддержку поставщикам услуг правительства Украины, включая правительственные министерства и операторов критической инфраструктуры, для выявления вредоносного ПО и восстановления систем после инцидентов.
- USAID предоставил более 6750 устройств экстренной связи, включая спутниковые телефоны и терминалы данных, поставщикам основных услуг, государственным чиновникам и операторам критически важной инфраструктуры в ключевых секторах, таких как энергетика и телекоммуникации.
- Агентство кибербезопасности и безопасности инфраструктуры (CISA) поделилось технической информацией об угрозах кибербезопасности.
- До февраля 2022 года правительство США тесно сотрудничало с министерствами правительства Украины и критически важными секторами инфраструктуры для поддержки киберустойчивости Украины, в том числе предоставив с 2017 года помощь в развитии киберпотенциала на сумму более 40 миллионов долларов США.

В июне 2022 года Глава американского киберкомандования США генерал Пол Накасоне, который одновременно является главой АНБ, выступая на конференции Центра кибероборонны НАТО в Таллине, ***впервые официально признал, что США проводили наступательные кибероперации***, а также информационные операции в поддержку Украины. Подробности операций не раскрыты, но Накасоне заявил, что они были законными и проводились под гражданским контролем и в соответствии с утверждённой в Минобороны США политикой.

Ранее представители США в публичных сообщениях подчёркивали, что в киберпространстве они помогают Украине только в оборонительном плане. Например, путём направления так называемых поисковых команд (hunt forward teams), которые вместе с местными специалистами занимались поиском угроз.

[32] «U.S. Support for Connectivity and Cybersecurity in Ukraine», U.S. Department of State, 2022.

Одним из ключевых аспектов работы Киберкомандования является так называемая «опережающая охота» (hunt forward). По словам Накасоне, специалисты киберкомандования были отправлены в 16 стран-союзников США, где они смогли получать разведданные из их компьютерных сетей, что «позволяет выявлять иностранных хакеров и идентифицировать их инструменты до того, как они будут использованы против США».

Во время одной из таких операций американские военные специалисты находились на Украине. «Мы поехали в декабре 2021 года по приглашению киевского правительства «поохотиться» вместе с ними. Мы пробыли там почти 90 дней», — сказал генерал. Представитель подтвердил, что эта группа была выведена в феврале 2022 года вместе с другими сотрудниками Министерства обороны США перед началом специальной военной операции[33].

Киберкомандование также сотрудничает с ведущими ИТ-организациями США, включая Microsoft. Эта компания не впервые делает заявления политического характера (например, после инцидента с атакой на Solar Winds президент Microsoft выступил с обвинениями России и сказал о том, что они разработают вместе с Правительством США меры противодействия), а также выделяет специалистов для кибероперациий на Украине. Подробнее о деятельности и заявлениях Microsoft можно прочесть в статье главного редактора BISA[34].

Также в июне 2022 стало известно, что представители компании L3Harris, подрядчика Пентагона, в течение последних месяцев несколько раз посещали Израиль с целью покупки NSO Group, известной шпионским ПО Pegasus. Любопытно то, что только в ноябре 2021 года администрация Байдена добавила NSO Group в список компаний, с которыми американским компаниям запрещено сотрудничать из соображений национальной безопасности.

Российская Федерация

В 2017 году министр обороны РФ Сергей Шойгу заявил о создании о создании в составе Вооруженных сил Российской Федерации **войск информационных операций.**

Исходя из опубликованных материалов, основными задачами этого формирования являются управление и ***защита военных компьютерных сетей, защита российских военных систем управления и связи от кибератак и надежное прикрытие проходящей по ним информации***[35].

[33] «Кибербезопасность, киберпреступность и кибервойны. Прошёл год»: https://bisa.ru/glavred-bdit/kiberbezopasnost-kiberprestupnost-i-kibervoyny-proshyol-god
[34] Там же.
[35] «Шойгу объявил о создании войск информационных операций», Российская Газета, 2017.

Соединенное Королевство

Стоит повторить, что в новой Стратегии кибербезопасности обозначен курс на наступательные кибервозможности Соединенного Королевства, наличие Национальной наступательной киберпрограммы и создание Национальных киберсил (NCF). Подробнее об этом было сказано в разделе 4.1.

Генеральный прокурор Соединенного Королевства заявил, что **страна может использовать «оборонительные кибератаки» против национальных государств,** когда «ключевые службы» (такие как критически важная инфраструктура и банки) подвергаются атаке со стороны иностранных злоумышленников[36].

Австралия

В Австралии существует подразделение Defence Science and Technology Group, которое создано для решения проблем обороны и национальной безопасности. *«Наша роль заключается в тесном сотрудничестве с австралийской экосистемой науки, технологий и инноваций для предоставления научных рекомендаций и решений, которые обеспечивают расширение возможностей для обороны и сообщества национальной безопасности»*[37].

Официально создано подразделение **Cyberwarfare Operations[38], в которое входят несколько групп:**

Группа Trustworthy Military Systems проводит исследования и разработки для выявления и противодействия воздействию недоверенных компонентов ИКТ, поддерживая правильную работу критически важных киберсистем ПВО.

Группа Counter Cyber Threats занимается исследованиями и разработками, чтобы выявлять и устранять угрозы для ключевой кибертерритории (cyber terrain) Их работа поддерживает кибероперации ПВО, уделяя особое внимание защите систем военных миссий и платформенных систем.

Группа Cognitive Cyber Security занимается исследованиями и разработками в области использования когнитивных подходов для автономной кибербезопасности, чтобы поддерживать кибероперации ADF своевременной защитой кибертерритории.

Группа Mission Protection and Effects занимается исследованиями и разработками концепций, технологий и методов для понимания текущего и прогнозируемого состояния собственных и угрожающих киберфизических систем.

КНР

Согласно заявлениям СМИ, в структуре Народно-освободительной армии Китая (НОАК) существует специальное **подразделение 61398**, численностью порядка 2 тысяч человек, предназначенное для проведения кибератак на компьютерные сети противника.

---

[36] «Defensive Cyber Attacks Declared Legal by UK AG, Path Cleared to "Hack Back" When Critical Infrastructure & Services Attacked», 06.06.2022.
[37] Australian Government, Department of Defence: Defence Science and Technology Group.
[38] Australian Government, Department of Defence: Cyberwarfare Operations.

По оценкам экспертов, на Генеральный штаб НОАК неформально работает и крупная хакерская группировка Red Hacker Alliance, которая насчитывает порядка 80 тысяч человек и состоит из членов китайской диаспоры со всего мира.

Само же правительство КНР всегда отрицало свою причастность к актам кибершпионажа и кибератак.

Иран

С 2010 года в Иране существует Командование кибероборонь (The Cyber Defense Command). Относится к Организации гражданской обороны (Passive Civil Defense Organization), который входит в Объединенный штаб вооруженных сил Ирана (Joint Staff of Iranian Armed Forces).

Идея создания Командования была выдвинута должностными лицами Организации гражданской обороны гораздо раньше, но убедить высшее руководство одобрить создание такой организации удалось лишь только после того, как иранские ядерные объекты подверглись атаке со стороны вредоносной программы Stuxnet.

В прессе различных стран, прежде всего США, опубликовано много статей о киберармии Ирана, но до сих пор этому нет ни одного официального подтверждения.

КНДР

Официальные заявления о создании кибервойск в КНДР в открытом доступе отсутствуют, равно как и информация о Стратегии кибербезопасности.

Однако согласно открытым публикациям, сделанным на основе интервью с бывшим военным КНДР, в стране существует подразделение по проведению кибероперацій под названием «Бюро 121», которое подчиняется Главному штабу по разведке и состоит из высококвалифицированных специалистов. По состоянию на 2014 год численность подразделения составляла порядка 1800 человек[39].

Южная Корея

В конце 2009 года Южная Корея заявила, что Министерство национальной обороны создаст киберкомандование (Cyber Warfare Command). Согласно заявлению, командование будет проводить не только оборонительные, но и наступательные операции[40].

Также по утверждению южнокорейских источников, подразделение по ведению наступательных операций в киберпространстве давно существует и в КНДР.

Франция

В 2019 году министр обороны Франции Флоренс Парли объявила о создании доктрины «Наступательные военные действия в киберпостранстве» («Militaire de lutte informatique. Offensive»)[41].

Большая часть документа засекречена, но он является руководством в области наступательного компьютерных операций.

---

[39] «In North Korea, hackers are a handpicked, pampered elite», Reuters, 2014.
[40] «Cyber Warfare Command to Be Launched in January», The Korea Times, 2009.
[41] «France unveils its doctrine for Offensive Computer Fight», Army Recognition, 2019.

В документе введен термин «**кибернаступление**» и заявлен принцип активного его применения в рамках военных действий. Министерство обороны Франции признало, что наступательные операции в киберпространстве стали полноценной составляющей вооруженных сил.

Израиль

В Израиле проведением операций в киберпространстве занимается **подразделение 8200**, которое входит в структуру военной разведки. ***По функциям является аналогом американского Агентства национальной безопасности и насчитывает несколько тысяч человек личного состава***[42].

Согласно заявлению эксперта по вопросам кибервойны Израиля, генерал-майора Исаака Бен Исраэля, готовность Израиля к военным действиям в киберпространстве, включая и оборону, и наступление, является одним из новых направлений в их планах.

Первый случай применения военной силы в ответ на кибератаку, приведшую к гибели людей, произошел 5 мая 2019 года: Силы обороны Израиля взорвали здание, в котором предположительно размещалась действующая хакерская группа ХАМАС[43].

Сингапур

В марте 2022 года Сингапур заявил о создании еще одного подразделения вооруженных сил наряду с сухопутными, воздушными и морскими — собственной **цифровой разведывательной службы**[44]. Сингапур, таким образом, стремится *«создать эффективную и модернизированную армию, которая сможет свести к минимуму его уязвимость и максимизировать его сильные стороны»*.

Министр обороны Сингапура подтвердил необходимость создания новой цифровой службы, сославшись на российско-украинский конфликт[45].

Украина

По прямым и косвенным признакам действия Украины в киберпространстве характеризуются:

- заявлением в новой Стратегии кибербезопасности о создании кибервойск в составе Министерства обороны Украины для совершения операций в киберпространстве и обеспечение их надлежащими финансовыми, кадровыми и техническими ресурсами для сдерживания вооруженной агрессии в киберпространстве и предоставления отпора агрессору;
- наличием «киберармии», в которую приглашаются все желающие;
- взаимодействием с Microsoft и АНБ еще до начала спецоперации, о чем в статье писал главный редактор BISA[46].

Также из открытых источников известно о создании подразделений по наступательным операциям в киберпространстве у Эстонии, Германии, Сирии.

---

[42] Bamahane — еженедельный журнал Армии обороны Израиля (АОИ).
[43] «What Israel's Strike on Hamas Hackers Means For Cyberwar», Wired, 2019.
[44] «Singapore's Military Modernization Program Is Ambitious – but Feasible», The Diplomat, 2022.
[45] Speech by Minister for Defence, Dr Ng Eng Hen, at the Committee of Supply Debates, 2022.
[46] «Кибербезопасность, киберпреступность и кибервойны. Прошёл год»: https://bisa.ru/glavred-bdit/kiberbezopasnost-kiberprestupnost-i-kibervoyny-proshyol-god

Индексы

В данном разделе мы опубликуем выдержки из других индексов и исследований, связанных с определением оборонительного и наступательного потенциала государств в киберпространстве.

В прошлом году мы выпустили исследование «Цифровизация и кибербезопасность», в котором писали о существующих индексах цифровизации и кибербезопасности[47].

Например, в **Глобальном индексе кибербезопасности** (Разработчик: Международный союз электросвязи при ООН) по итогам 2020 года Российская Федерация заняла 5 место:

Таблица 1

Country Name	Score	Global Cybersecurity Index 2020 Rank
United States	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5

Источник: ITU Cybersecurity Index 2021

Далее мы кратко рассмотрим 2 новых индекса.

National Cyber Power Index[48]

База данных «Harvard Belfer National Cyber Power Index 2020 (NCPI 2020)» включает информацию о **кибервозможностях**, **кибернамерениях** и **кибермощности 30 стран в 2020 г.**

Национальный индекс кибермощности (NCPI 2020) который является комбинацию Индекса кибервозможностей (CCI) и Индекса кибернамерений (CII).

По словам авторов исследования, кибермогущество государства состоит из нескольких компонентов и должно рассматриваться в контексте национальных целей страны.

NCPI определил семь национальных целей, которые страны преследуют с помощью киберсредств:

1. Наблюдение и мониторинг.
2. Укрепление и совершенствование национальной кибербезопасности.
3. Контроль и манипулирование информационной средой.

[47] Аналитический отчет InfoWatch «Цифровизация и киберезопасность»: https://www.infowatch.ru/analytics/analitika/kak-otsenivat-urovni-tsifrovizatsii-i-kiberbezopasnosti

[48] Harvard Belfer National Cyber Power Index 2020.

4. Сбор внешней разведывательной информации для национальной безопасности.
5. Коммерческая прибыль или рост отечественной промышленности.
6. Уничтожение или вывод из строя инфраструктуры и возможностей противника.
7. Определение международных норм в киберпространстве и технических стандартов.

Первой 10-кой стран по итогам исследования стали:

Таблица 2

#	Country	Overall score	Capability	Intent
1	United States	50.24	1	2
2	China	41.47	2	1
3	United Kingdom	35.57	3	3
4	**Russia**	**28.38**	**10**	**4**
5	Netherlands	24.18	9	5
6	France	23.43	5	11
7	Germany	22.42	4	12
8	Canada	21.50	11	9
9	Japan	21.03	8	14
10	Australia	20.04	16	8

Источник: Harvard Belfer National Cyber Power Index 2020

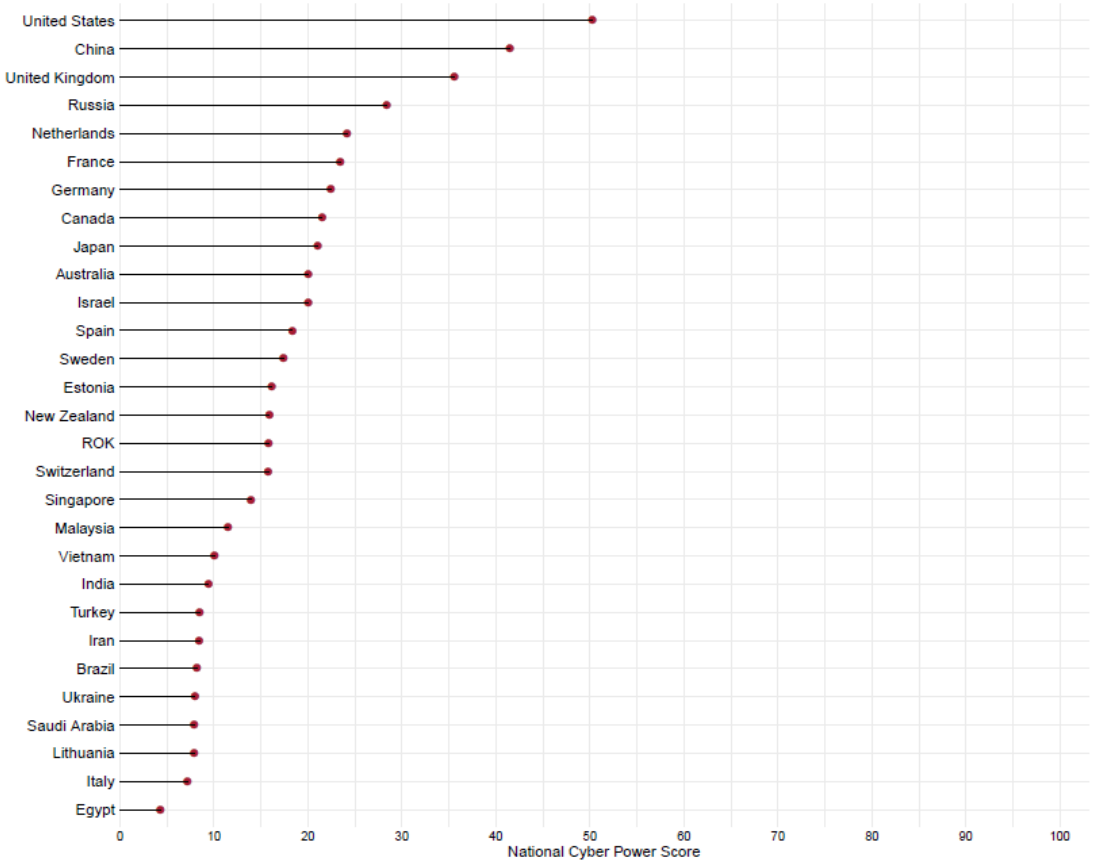

Рисунок 2. Самые всесторонне развитые киберсилы
(Источник: Harvard Belfer National Cyber Power Index 2020)

Рисунок 3
(Источник: Harvard Belfer National Cyber Power Index 2020)

Cyber Arms Watch[49]

Индекс Cyber Arms Watch пробует оценить прозрачность наступательных кибервозможностей 60 стран и сравнивает степень прозрачности заявленных государствами кибервозможностей с внешним восприятием этих возможностей.

Рейтинг заявленных возможностей (DCR) показывает, в какой степени государство публично раскрывает информацию о своих наступательных кибервозможностях. Сюда входят официальные правительственные сообщения, такие как стратегии, доктрины и аналогичные документы, а также сообщения средств массовой информации, которые в совокупности указывают уровень заявленных возможностей.

Рейтинг воспринимаемых возможностей (PCR) показывает, как наступательные кибервозможности государства наблюдают посторонние, используя информацию из открытых источников. В то время как Рейтинг заявленных возможностей (DCR) ограничен официальным раскрытием информации самим правительством, этот рейтинг описывает наступательные кибервозможности этого правительства с

[49] Cyber Arms Watch: An Analysis of Stated & Perceived Offensive Cyber Capabilities, 2022.

использованием внешних источников. Это разведывательные отчеты, обвинительные заключения, прошлые операции, утечки документов.

Инструмент Cyber Arms Watch Monitor — это интерактивное исследование набора данных Cyber Arms Watch на трех вкладках: заявленные возможности, предполагаемые возможности и окончательный индекс прозрачности.

Самыми «непрозрачными» странами по мнению авторов индекса стали:

- КНДР;
- Иран;
- Российская Федерация.

По рейтингу заявленных кибервозможностей Российская Федерация получила 0 баллов, в то время как по Рейтингу воспринимаемых возможностей (PCR) заработала максимальные 5 баллов.

Самыми «прозрачными» странами стали США, Австралия, Франция и Норвегия.

Общий результат исследования выглядит следующим образом:

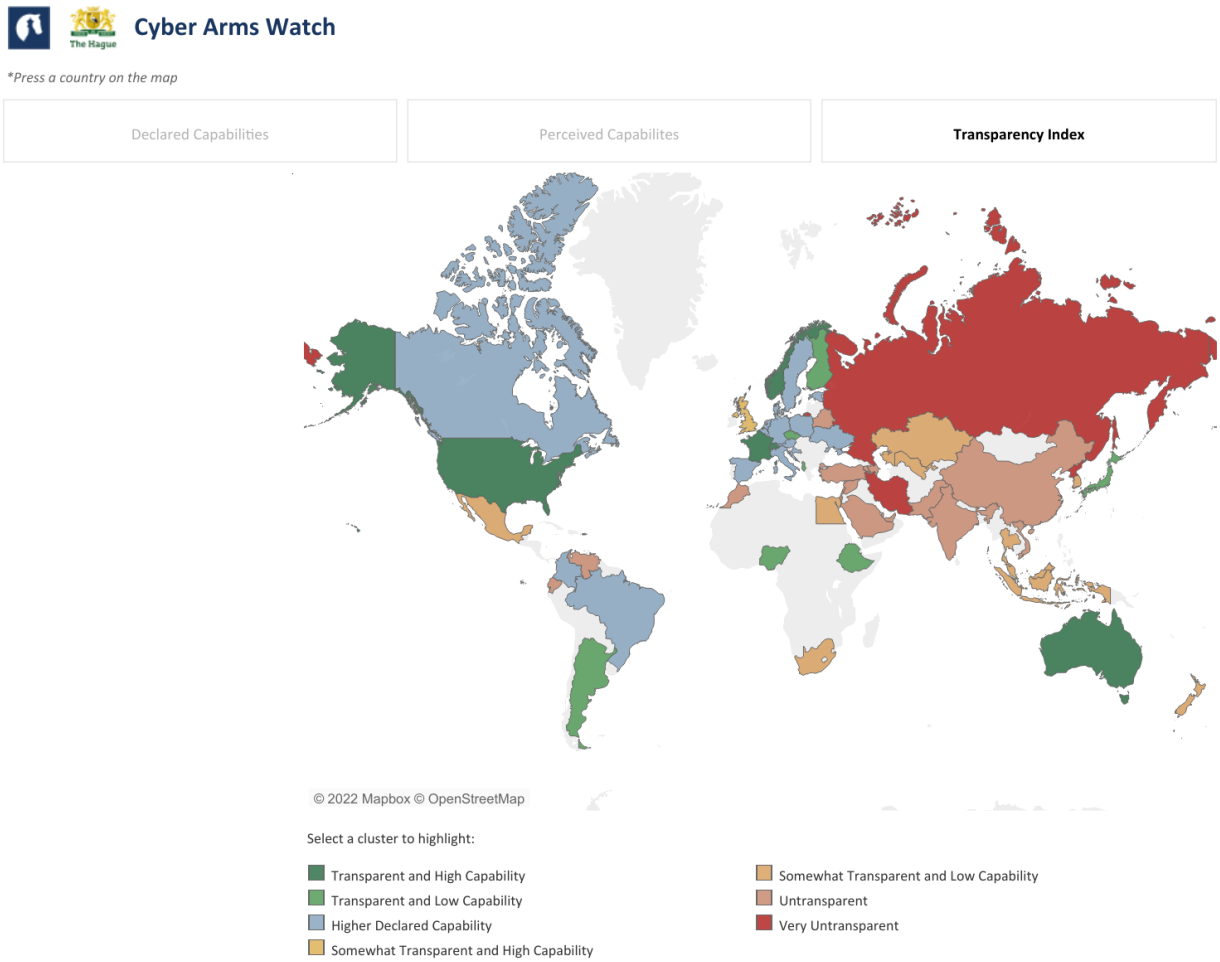

Рисунок 4

(Источник: Cyber Arms Watch: An Analysis of Stated & Perceived Offensive Cyber Capabilities, 2022)

Выводы

Мы видим, что кибербезопасность становится важным, если не ключевым элементом национальной безопасности, как для стран с развитой цифровой экономикой (США, Канада, Австралия), так и для тех, кто только встал на путь цифровизации. Более чем у ста государств разработаны собственные стратегии кибербезопасности. Например, такой документ есть также у Фиджи, Нигерии, Гватемалы и Никарагуа.

Стратегия кибербезопасности по факту является документом, фиксирующим и определяющим государственную политику, направленную на обеспечение безопасности государства (отрасли, направления) в киберпространстве.

Для обзора выбраны и проанализированы стратегии 10 стран, кроме того, мы ознакомились со стратегиями Южной Кореи, Сингапура и Индии. У некоторых интересующих нас государств документы в отношении кибербезопасности отсутствуют в открытом доступе — например, у Ирана и КНДР.

В данном исследовании рассмотрены содержание и цели стратегий кибербезопасности, выявлены сходства и различия в стратегиях ряда интересующих нас стран. Чтобы полностью проанализировать какую-либо из стратегий, понадобится отдельный отчет, как это было сделано Экспертно-аналитическим центром InfoWatch с обзором стратегии кибербезопасности Японии. В дальнейшем мы, возможно, опубликуем аналитику документов отдельных государств.

Стратегии кибербезопасности имеют ряд сходств и различий.

Стратегии схожи по целям, поскольку обеспечение кибербезопасности стало приоритетным направлением обеспечения национальной безопасности государств и их критически важных отраслей. Все страны обеспокоены безопасностью киберпространства, включающего в себя критическую информационную инфраструктуру (сети связи, ИС, АСУ, IoT и т.д.), а противником в большинстве стратегий признается киберпреступность. Поднимаются вопросы сотрудничества в борьбе с киберпреступностью, единодушно отмечается эволюция киберугроз, а также отмечается необходимость совместной работы и международного регулирования действий в киберпространстве. Австралия и Канада, например, в своих стратегиях опубликовали размеры инвестиций в кибербезопасность.

Различия же состоят в:

- ✓ Структуре. Имея общую идею (безопасность в киберпространстве), каждая стратегия уникальна по своей структуре.
- ✓ Наличии заявлений о намерениях стать кибердержавой. Например, это присутствует в стратегиях США и Китая.
- ✓ Характере заявленных методов действий. Стратегии сконцентрированы не только на оборонительных действиях, но и заявляют о наступательных мерах, а в некоторых случаях и о создании новых подразделений вооруженных сил, включающих силы кибероперациий. К содержащим наступательные методы в стратегиях кибербезопасности относятся США, Соединенное Королевство, Украина.

- ✓ Заявлениях о противниках и конкурентах в киберпространстве — у всех противником обозначена киберпреступность, но у ряда стран дополнительно названы национальные государства, в ряде случаев указано, какие именно.

Некоторые государства (США, Соединенное Королевство) открыто критикуют политику в киберпространстве других государств.

Стратегии России и Китая акцентированы на сохранении собственного суверенитета в киберпространстве, при этом в стратегии США такое понятие отсутствует, а в предисловии американской киберстратегии, наоборот, сказано, что Китай и Россия — конкуренты и противники США в киберпространстве, что они «прикрываются» понятиями суверенитета и наносят экономический ущерб США, «отдельным лицам, коммерческим и некоммерческим интересам и правительствам по всему миру».

В Стратегии Соединенного Королевства также критикуются Россия и Китай за их стремление к суверенитету в киберпространстве.

В Стратегии кибербезопасности Украины тоже звучит критика стремления к суверенности в киберпространстве, при этом в самой Стратегии неоднократно встречаются фразы о собственном государственном суверенитете.

Анонс новой стратегии Японии и новой редакции Таллинского руководства НАТО предусматривают позиционирование Российской Федерации как угрозы их безопасности.

В то же время, киберпространство стало новым полем боя (пространством ведения боевых действий). При этом стоит заметить, до сих пор отсутствуют общепринятые международные правила поведения в киберпространстве и множество стран в своих стратегиях кибербезопасности обеспокоены данным вопросом.

Таллинское руководство пусть и пытается установить правила проведения киберконфликтов, но даже в экспертном сообществе, которое его составляло, возникали споры по поводу того или иного правила. На международном уровне не утверждено никаких конкретных правил по поводу установления ответственности государства за кибератаки. К тому же, практически невозможно определить и приписать атаку конкретному государству.

При этом многие сосредоточены на наращивании не только оборонного, но и наступательного потенциала.

По официальным и неофициальным данным, подразделения по проведению кибероперациий есть в США, Соединенном Королевстве, Франции, КНР, Израиле и других государствах.

Официально о подразделениях для проведения кибероперациий заявили немногие страны, но есть все основания полагать, что такими подразделениями обладает куда большее количество государств. Например, отсутствие официальной информации о кибервойсках КНДР и Ирана не говорит о том, что таких войск нет.

Все вышесказанное вызывает серьёзные опасения. Перекос от оборонительной к наступательной политике в сфере обеспечения кибербезопасности может спровоцировать глобальный конфликт, от которого пострадают все государства не только в цифровом пространстве, но и в реальном мире.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

Почтовая рассылка

VKontakte https://vk.com/infowatch

Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics