РУКОВОДСТВО ПО РАЗРАБОТКЕ НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

СТРАТЕГИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

ITU

CCDCOE

The Commonwealth Cybercrime Initiative

CTO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Deloitte.

Global Cyber Security Capacity Centre

GCSP

Microsoft

POTOMAC INSTITUTE FOR POLICY STUDIES

Часть прав защищена

Права и разрешения

Адаптация – При адаптации этой работы следует добавить к ссылке на источник следующую оговорку: "*Эта публикация представляет собой адаптацию оригинальной работы*, авторами которой являются Международный союз электросвязи (МСЭ), Всемирный банк, Секретариат Содружества (Comsec), Организация электросвязи Содружества (СТО) и Экспертный центр НАТО по совместной кибероборонe (NATO CCD COE). *Вышеупомянутые организации не выражали своей поддержки высказанным в этой адаптации взглядам и мнениям, исключительную ответственность за которые несут автор или авторы адаптации*".

Заимствованные материалы – Международный союз электросвязи (МСЭ), Всемирный банк, Секретариат Содружества (Comsec), Организация электросвязи Содружества (СТО) и Экспертный центр НАТО по совместной кибероборонe (NATO CCD COE) необязательно являются собственниками всех компонентов содержащихся в данной работе материалов. Соответственно, они не гарантируют, что использование каких-либо отдельных компонентов или материалов, принадлежащих третьим сторонам и содержащихся в этой работе, не будет являться нарушением прав этих третьих сторон. Исключительная ответственность за риски, связанные с возможностью предъявления претензий в результате такого нарушения, лежит на вас. Если вы хотите повторно использовать какой-либо компонент этой работы, вы обязаны определить, необходимо ли разрешение для такого повторного использования, и получить его у владельца авторских прав. Примеры таких компонентов включают, среди прочего, таблицы, статистические данные или изображения.

Любые просьбы об использовании этой работы в целях, выходящих за рамки вышеупомянутой лицензии (CC BY 3.0 IGO), следует направлять в Международный союз электросвязи (МСЭ), Place des Nations, 1211 Geneva 20, Switzerland; эл. почта: itumail@itu.int.

Выражение признательности

Настоящее руководство было разработано двенадцатью партнерами, представляющими межправительственные и международные организации, частный сектор, а также академические организации и гражданское общество, а именно: Секретариат Содружества (Comsec), Организация электросвязи Содружества (CTO), компания Deloitte, Женевский центр политики безопасности (ЖЦПБ), Глобальный центр создания потенциала в области кибербезопасности (GCSCC) при Оксфордском университете, Международный союз электросвязи (МСЭ), компания Microsoft, Экспертный центр НАТО по совместной кибероборонe (NATO CCD COE), Потомакский институт политических исследований, Исследовательский центр RAND Europe, Всемирный банк и Конференция Организации Объединенных Наций по торговле и развитию (ЮНКТАД).

В редакционную группу вошли Каталайна Саполу (Comsec), Шадрах Харуна (Comsec), Мартин Койябе (CTO), Фаргани Тамбеайюк (CTO), Андреа Ригони (Deloitte), Каролин Вайсер (GCSCC), Марко Обисо (МСЭ), Каджа Сиглич (Microsoft), Кадри Каска (NATO CCD COE), Франческа Спидальери и Мелисса Хатауэй (Потомакский институт политических исследований), Эрик Силфверстен (RAND Europe), Давид Сатола и Сандра Серджент (Всемирный банк) и Сесиль Барейр (ЮНКТАД).

Значительный вклад в подготовку сборника внесло также Агентство по сетевой и информационной безопасности Европейского союза (ENISA).

Хотелось бы отметить также вклад следующих лиц: Грейс Акайо, Рошин Авотар-Маури, Бен БейслиУокер, Пол Корниш, Люк Дандюран, Майкл Голдсмит, Кемаль Хусейнович, Андраж Анди Кастелич, Максим Куштуев, Лена Латтион, Густав Линдстром, Дамьен Маддалена, Эмили Мунро, Лара Пейс, Сара Пуэльо Альфонсо, Валерия Рисулья, Тейлор Робертс, Моника М. Руис, Ирен Рубио, Энн Вальятага, Джулиенн Райт.

Вступление

Имею честь представить вам от имени всех участвовавших в подготовке этой публикации партнеров "Руководство по разработке национальной стратегии кибербезопасности", цель которого заключается в том, чтобы предложить совокупный и согласованный набор принципов и примеров передового опыта, касающихся разработки, принятия и применения национальных стратегий кибербезопасности.

Двенадцать партнеров, представляющих государственный и частный секторы, академические организации и гражданское общество, договорились при содействии МСЭ поделиться своим опытом, знаниями и экспертным анализом, подготовив руководство, в котором собраны практические методы, используемые участвующими в этом сборнике организациями, а также ссылки на дополнительные публикации, в целях упрощения доступа к имеющимся ресурсам.

В последние два десятилетия миллиарды людей во всем мире смогли воспользоваться преимуществами экспоненциального роста и стремительного внедрения информационно-коммуникационных технологий, а также связанными с этим социально-экономическими возможностями. Мы живем в эпоху цифровой революции, которая ведет к коренным преобразованиям в нашем обществе.

Кибербезопасность является одним из основных факторов обеспечения социально-экономического развития. В то же время всего лишь 67 стран мира[1] имеют находящиеся в открытом доступе национальные стратегии кибербезопасности. В связи с этим решительно необходимо стимулировать деятельность по их разработке. Как видно из названия, цель этого Руководства заключается в том, чтобы дать импульс стратегическому мышлению и помочь руководству стран и директивным органам в разработке, принятии и применении национальных стратегий кибербезопасности.

Я убежден в том, что Руководство по разработке национальной стратегии кибербезопасности станет полезным инструментом для всех заинтересованных сторон, выполняющих функции, связанные с кибербезопасностью. Я хотел бы лично выразить признательность партнерам за их неизменные и неоценимые поддержку и приверженность успешному завершению этого проекта, который должен стать конкретным примером плодотворного сотрудничества с участием многих заинтересованных сторон.

Брахима Сану
Директор Бюро, электросвязи МСЭ

[1] По данным Глобального индекса кибербезопасности МСЭ (GCI) за 2017 год.

Содержание

Предисловие

Настоящее Руководство по разработке национальной стратегии кибербезопасности представляет собой один из наиболее полных обзоров различных элементов успешных стратегий кибербезопасности. Это результат уникального, совместного и равноправного труда многих заинтересованных сторон, в котором использованы знания, опыт и экспертный анализ многочисленных организаций в области национальных стратегий и политики кибербезопасности. Данное Руководство было подготовлено двенадцатью партнерами, представляющими государственный и частный секторы, а также академические организации и гражданское общество.

Эти партнеры объединили свои усилия, исходя из необходимости укрепления в международном сообществе сотрудничества и координации по вопросам создания потенциала в области кибербезопасности. Эти усилия направлены на поддержку руководства стран и директивных органов в разработке защитных мер реагирования на киберугрозы, которые могут быть сформулированы в виде национальной стратегии кибербезопасности, а также в стратегическом осмыслении вопросов кибербезопасности, обеспечения готовности к киберугрозам, реагирования на них и устойчивости к ним путем укрепления доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ).

Руководство по разработке национальной стратегии кибербезопасности было подготовлено на основе цикличного подхода, направленного на достижение соглашения путем выстраивания консенсуса. Оно основано на существующих ресурсах и направлено на содействие их использованию заинтересованными сторонами на национальном уровне. При возможности, перечень соответствующих источников и инструментов, использовавшихся для разработки каждого набора рекомендаций, включался в раздел "Справочные материалы" для поощрения их более широкого использования.

Кибербезопасность – это фундаментальный компонент, лежащий в основе достижения социально-экономических целей современной экономики. Мы рассчитываем, что настоящее Руководство по разработке национальной стратегии кибербезопасности будет полезным инструментом для всех заинтересованных сторон, включая национальные директивные, законодательные и регуляторные органы, на которые возложены функции по обеспечению кибербезопасности. Кроме того, это Руководство может иметь более широкое применение, поскольку представленные в нем принципы могут применяться на региональном или муниципальном уровне, а также быть адаптированы для целей отрасли.

1 Краткий обзор документа

1.1 Цель

Цель настоящего документа заключается в том, чтобы предоставить руководству и директивным органам стран руководящие указания по разработке национальной стратегии кибербезопасности и стратегическому осмыслению вопросов кибербезопасности, готовности и устойчивости к киберугрозам.

В настоящем Руководстве содержится полезная, гибкая и удобная для использования рамочная структура, которая может использоваться для определения исходных условий: концепции социально-экономического развития страны и текущей доктрины в области безопасности, а также для помощи директивным органам в разработке стратегии, учитывающей конкретное положение дел в стране, культурные и общественные ценности и поощряющей построение безопасных, способных к восстановлению, наделенных инструментами ИКТ и соединенных обществ.

Данное Руководство является уникальным ресурсом, поскольку в нем содержится структура, согласованная организациями, обладающими подтвержденным и разнообразным опытом в этой актуальной области, и составленная на основе результатов их работы в этой сфере. Таким образом, в нем представлен наиболее полный на настоящий момент обзор компонентов успешных национальных стратегий кибербезопасности.

1.2 Сфера применения

Обеспечение кибербезопасности – это комплексная задача со множеством различных управленческих, политических, эксплуатационных, технических и правовых аспектов. В настоящем Руководстве предпринята попытка рассмотрения, организации и расстановки в порядке приоритетности многих из этих областей на основе существующих и получивших широкое признание моделей, рамочных структур и других справочных материалов.

Основное внимание в настоящем Руководстве уделяется защите гражданских аспектов киберпространства, поэтому в нем выделены всеобъемлющие принципы и примеры передового опыта, которые следует учитывать в процессе разработки и написания национальной стратегии кибербезопасности, а также руководства ее применением.

В этих целях в Руководстве четко разграничены "процесс", которому страны будут следовать на протяжении всего жизненного цикла национальной стратегии кибербезопасности (инициирование, обзор и критический анализ имеющегося опыта, разработка, осуществление, пересмотры), и "содержание", т. е. конкретный текст документа с национальной стратегией кибербезопасности. В Руководстве не освещены такие аспекты, как создание оборонительного или наступательного киберпотенциала вооруженных сил страны, сил обороны или разведывательных управлений, хотя целый ряд стран работает над созданием такого потенциала.

Цель настоящего Руководства заключается в том, чтобы предоставить руководящие указания и привести примеры передового опыта, касающиеся компонентов, которые следует включить в национальную стратегию кибербезопасности, а также того, как ее разрабатывать, применять и пересматривать, поэтому в нем рассматриваются оба этих аспекта.

В Руководстве также приведен обзор ключевых компонентов обеспечения готовности страны к киберугрозам и отмечены критически важные аспекты, которые следует учитывать правительствам при разработке своих национальных стратегий и планов осуществления.

Наконец, в настоящем Руководстве директивным органам предлагается всеобъемлющий обобщенный обзор существующих подходов и приложений, а также приводятся ссылки на дополнительные и вспомогательные ресурсы, которые могут использоваться при подготовке конкретных мер по обеспечению кибербезопасности, принимаемых на национальном уровне.

1.3 Общая структура и использование Руководства

Настоящее Руководство составлялось, в первую очередь, в качестве вспомогательного ресурса для заинтересованных сторон из числа государственных органов, чтобы они могли его использовать при подготовке и написании их национальной стратегии кибербезопасности, а также в процессе руководства ее применением. Соответственно, его структура была разработана в соответствии с процессом и порядком разработки стратегии:

- Раздел 2 – Введение: обзор основной темы Руководства и соответствующие определения;
- Раздел 3 – Жизненный цикл разработки стратегии: подробное описание этапов разработки стратегии и руководства ее применением на протяжении всего жизненного цикла;
- Раздел 4 – Всеобъемлющие принципы, лежащие в основе стратегии: сквозные базовые соображения, которые следует учитывать в ходе разработки стратегии;
- Раздел 5 – Тематические области и передовой опыт: определение ключевых элементов и тем, которые следует учитывать при разработке стратегии;
- Раздел 6 – Вспомогательные справочные материалы: дополнительные ссылки на литературу по данной тематике, которую заинтересованные стороны могут рассмотреть в процессе написания текста.

В частности, в Разделе 3 описывается процесс разработки национальной стратегии кибербезопасности (подготовка, написание, осуществление и обеспечение устойчивости в долгосрочной перспективе) и связанные с ним аспекты, а в Разделах 4 и 5 большее внимание уделяется содержанию национальной стратегии кибербезопасности, поскольку в них освещены понятия и компоненты, которые должен содержать этот документ.

1.4 Целевая аудитория

Настоящее руководство предназначено, прежде всего, для директивных органов, ответственных за разработку национальной стратегии кибербезопасности. Во вторую очередь оно адресовано всем остальным заинтересованным сторонам из государственного и частного секторов, участвующим в процессе разработки и осуществления стратегии, таким как ответственные сотрудники государственных органов, представители регуляторных и правоохранительных органов, поставщики услуг ИКТ, операторы важнейшей инфраструктуры, представители гражданского общества, академических организаций и исследовательских учреждений. Руководство также может быть полезно различным заинтересованным сторонам из международного сообщества в сфере развития, которые оказывают помощь в обеспечении кибербезопасности.

2 Введение

В последние два десятилетия миллиарды людей во всем мире смогли воспользоваться преимуществами экспоненциального роста и стремительного внедрения информационно-коммуникационных технологий, а также связанными с этим социально-экономическими возможностями.

С момента своего создания интернет прошел путь развития от платформы обмена информацией до основополагающего элемента современного бизнеса, важнейших услуг и инфраструктуры, социальных сетей и мировой экономики в целом. В результате этого руководители стран начали внедрять цифровые стратегии и финансировать проекты, способствующие расширению возможностей установления интернет-соединений и задействующие преимущества использования ИКТ в целях стимулирования экономического роста, повышения производительности и эффективности, усовершенствования процесса оказания услуг и наращивания потенциала, обеспечения доступа к предпринимательской деятельности и информации, создания условий для электронного обучения, повышения квалификации работников и содействия надлежащему управлению. Страны не могут пренебрегать возможностями, связанными с обеспечением соединения и участия в экономике, основанной на интернете.

Хотя наши общества все больше используют цифровую инфраструктуру, технологии по сути своей остаются уязвимыми. Конфиденциальность, целостность и доступность инфраструктуры ИКТ подвергаются опасности в виде стремительно изменяющихся киберугроз, включая электронное мошенничество, кражу интеллектуальной собственности и информации, позволяющей установить личность, перебои в обслуживании и нанесение ущерба собственности или ее разрушение. Преобразовательные возможности ИКТ и интернета в качестве катализаторов экономического роста и социального развития находятся на критическом этапе, когда доверие и уверенность граждан и стран в целом при использовании ИКТ ослабляются в результате незащищенности киберпространства.

Для всестороннего использования потенциала технологий государствам следует согласовать свою национальную экономическую концепцию с национальными приоритетами в области безопасности. Если в противовес угрозам безопасности, связанным с повсеместным распространением инфраструктуры, функционирующей на основе ИКТ, и интернет-приложений, не будут приняты комплексные национальные стратегии кибербезопасности и планы обеспечения способности к восстановлению, страны не смогут обеспечить экономический рост и достичь поставленных перед собой целей национальной безопасности.

Реагируя на эти проблемы, государства создают как наступательный, так и оборонительный потенциал для защиты от запрещенной и незаконной деятельности в киберпространстве и предотвращения инцидентов прежде, чем они нанесут ущерб стране. В настоящем документе подробно рассматриваются ответные защитные меры, принимаемые, в частности, в форме национальных стратегий кибербезопасности.

Разработка и осуществление национальной стратегии кибербезопасности позволяет стране улучшить безопасность ее цифровой инфраструктуры и в конечном итоге способствует реализации ее более широких социально-экономических устремлений. Руководителям стран необходимо производить стратегический анализ возможностей и рисков, которые несет в себе цифровая среда для их стран; им также следует разработать четкую концепцию цифрового общества, которое они хотят создать.

2.1 Что такое кибербезопасность?

Существуют различные определения термина "кибербезопасность", сформулированные на национальном и международном уровнях. Для целей настоящего документа используется следующее значение термина "кибербезопасность": это набор средств, стратегии, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, передовой опыт, гарантии и технологии, которые могут быть использованы для защиты доступности, целостности и конфиденциальности ресурсов в соединенной инфраструктуре, используемой государственными органами, частными организациями и гражданами; такие ресурсы включают соединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и данные в киберсреде 2.

2.2 Преимущества национальной стратегии кибербезопасности и процесс разработки стратегии

Национальные стратегии кибербезопасности могут принимать различную форму и отличаться разными уровнями проработки деталей, в зависимости от целей и уровня готовности к киберугрозам каждой конкретной страны. Соответственно, не существует установленного и общепринятого определения элементов, которые составляют национальную стратегию кибербезопасности.

Настоящий документ составлен с учетом имеющихся результатов научных исследований в этой области; в нем заинтересованным сторонам рекомендуется рассматривать национальную стратегию кибербезопасности как:

- выражение концепции, целей, принципов и приоритетов высокого уровня, которыми руководствуется страна при обеспечении кибербезопасности;
- обзор заинтересованных сторон, которым поручено укрепление кибербезопасности страны, и их соответствующих функций и обязанностей;
- описание мер, программ и инициатив, которые страна будет реализовать для защиты своей национальной киберинфраструктуры и параллельного укрепления ее безопасности и способности к восстановлению.

[2] Определение составлено на основе адаптированного текста из следующего источника: https://www.bcmpedia.org/wiki/Cyber_Security

Определение концепции, целей и приоритетов дает правительствам возможность рассматривать проблему кибербезопасности в целом, в масштабе всей национальной цифровой экосистемы, а не в каком-либо отдельно взятом секторе, с точки зрения какой-либо задачи или необходимости реагирования на конкретный риск, что позволяет им мыслить стратегически. Приоритеты национальных стратегий кибербезопасности варьируются в зависимости от страны, поэтому в одной стране они могут уделять особое внимание реагированию на риски, связанные с важнейшей инфраструктурой, в то время как в других они могут быть нацелены на защиту интеллектуальной собственности, содействие обеспечению доверия в онлайновой среде или повышение осведомленности общественности в вопросах кибербезопасности, либо сочетать в себе эти задачи.

Для успешного контроля рисков в такой всеохватной области, как кибербезопасность, решающее значение имеет определение инвестиций и ресурсов и последующая расстановка их в порядке приоритетности.

Национальная стратегия кибербезопасности предоставляет также возможность согласования приоритетов в области кибербезопасности с другими целями, имеющими отношение к ИКТ. Кибербезопасность является основополагающим элементом достижения социально-экономических целей современной экономики, поэтому в стратегии следует отразить, каким образом оказывается поддержка их реализации. Это можно сделать путем ссылки на действующие политические меры, направленные на осуществление программ цифровизации или развития страны, или путем оценки возможностей включения в эти программы мер, касающихся кибербезопасности.

Наконец, в процессе разработки национальной стратегии кибербезопасности концепция правительства должна быть преобразована в согласованные и реализуемые политические меры, которые будут способствовать достижению ее целей. Это включает в себя не только меры, программы и инициативы, которые надлежит принять, но и выделенные на эту деятельность ресурсы и пути их использования. Аналогичным образом, в ходе этого процесса следует определить параметры, которые будут использоваться для проверки того, были ли достигнуты желаемые конечные результаты в рамках установленных бюджета и срока.

3 Жизненный цикл национальной стратегии кибербезопасности

В данном разделе содержится обзор различных этапов разработки стратегии, которые включают:

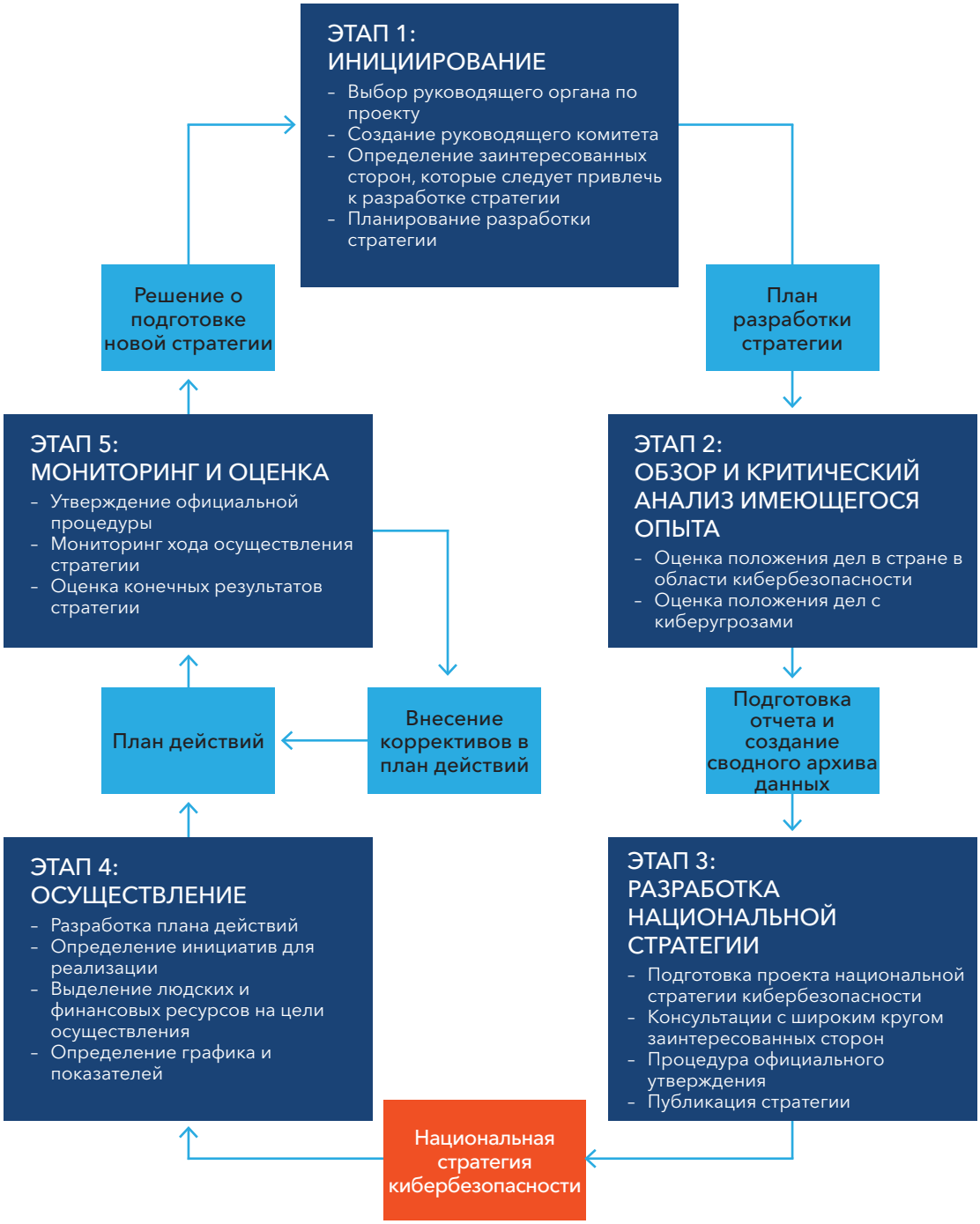
- Этап I – Инициирование
- Этап II – Обзор и критический анализ имеющегося опыта
- Этап III – Разработка
- Этап IV – Осуществление
- Этап V –Мониторинг и оценка

В этом разделе описаны также основные структуры, которые следует привлекать к участию в разработке стратегии, и перечислены другие соответствующие заинтересованные стороны, которые могут внести свой вклад в этот процесс.

В конечном итоге этот раздел нацелен на разъяснение читателю мер, которые следует принять на страновом уровне для разработки национальной стратегии, и возможных механизмов ее осуществления в соответствии с конкретными потребностями и требованиями страны, включая всеобъемлющие принципы (описанные в разделе 4) и передовой опыт (описан в разделе 5).

Читатели настоящего документа могут использовать показанный на Рисунке 1 жизненный цикл в качестве ориентира при стратегическом анализе кибербезопасности на национальном уровне.

Рисунок 1 – Жизненный цикл национальной стратегии кибербезопасности



3.1 Этап I: Инициирование

На этапе инициирования национальной стратегии кибербезопасности, который описан в разделах 4 и 5 настоящего документа, закладываются основы для ее эффективной разработки. Основное внимание на этом этапе должно уделяться процедурам, графикам и определению ключевых заинтересованных сторон, которые следует привлекать к разработке стратегии. Конечным результатом этого этапа является подготовка плана разработки стратегии. Если это предусмотрено государственным устройством страны, план может подаваться на утверждение высшему органу исполнительной власти[3] в этой стране.

3.1.1 Выбор руководящего органа по проекту

В соответствии с принципом четкого определения руководства, функций и распределения ресурсов (раздел 4.8), координацию процесса разработки стратегии должен осуществлять один компетентный орган власти. Высший орган исполнительной власти должен поручить руководство разработкой стратегии либо уже существующему, либо созданному для этих целей государственному органу, такому как министерство, управление или департамент. Эта структура, которая в настоящем документе именуется "руководящий орган по проекту", должна, в свою очередь, назначить конкретное лицо, ответственное за руководство процессом разработки стратегии и отчитывающееся по нему.

На протяжении всего процесса разработки стратегии руководящий орган по проекту должен сохранять нейтральность. В этих целях рекомендуется, чтобы за осуществление стратегии отвечал другой орган. Такой или иные механизмы следует использовать для того, чтобы предотвратить любую внутреннюю предвзятость и избежать внутриправительственного соревнования за ресурсы.

3.1.2 Создание руководящего комитета

Высший орган исполнительной власти также должен создать руководящий комитет, который будет заниматься разработкой стратегии вместе с руководящим органом по проекту. Он должен иметь полномочия для предоставления руководящих указаний, а также участвовать в контроле качества. Кроме того, он должен гарантировать прозрачный и открытый для всех характер процесса, в соответствии с принципом четкого определения руководства, функций и распределения ресурсов (раздел 4.8). Функции, структуру и членский состав руководящего комитета следует четко определить с самого начала.

Поскольку руководящий комитет может рассматривать конфиденциальные документы, его состав следует определить соответствующим образом. Важно также обеспечить, чтобы его членский состав соответствовал различным обязанностям, возложенным на этот орган, например, путем соблюдения иерархии назначений.

3.1.3 Определение заинтересованных сторон, которые следует привлечь к разработке стратегии

На этом этапе руководящему органу по проекту следует определить предварительный круг заинтересованных сторон, которые необходимо привлечь к разработке стратегии. Ему также необходимо четко определить функции различных заинтересованных сторон и описать механизмы их сотрудничества, с тем чтобы реагировать на их ожидания на протяжении всего процесса.

[3] Лицо или орган, руководящее процессом принятия решений на национальном уровне.

В ходе процесса разработки руководящему органу по проекту может понадобиться обратиться к новым заинтересованным сторонам для обеспечения использования всех знаний и экспертного опыта по данной тематике. Это соответствует принципу открытости для всех (раздел 4.3), в котором подчеркивается важное значение сотрудничества с широким кругом заинтересованных сторон, представляющих государственные органы, частный сектор и гражданское общество. Например, руководящий орган по проекту может рассмотреть возможность привлечения к этому процессу компаний, работающих в сфере ИКТ, операторов важнейшей инфраструктуры, академических экспертов и неправительственных организаций, занимающихся повышением осведомленности о кибербезопасности и обеспечением готовности, и других сторон.

Такой механизм сотрудничества может также принимать форму консультативного комитета, который будет участвовать в процессе путем включения своих членов в состав руководящего комитета, а также путем предоставления консультаций на различных этапах.

3.1.4 Планирование процесса разработки стратегии

На заключительном отрезке этапа инициирования руководящий орган по проекту должен подготовить план разработки национальной стратегии кибербезопасности. После составления плана его следует представить на утверждение руководящему комитету и высшему органу исполнительной власти, в зависимости от обстоятельств и в соответствии с национальными процедурами управления.

При составлении плана руководящему органу по проекту следует также рассмотреть вопрос о том, будет ли национальная стратегия кибербезопасности приниматься в форме закона или в форме политики, поскольку эти разные варианты могут повлиять на выбор официальных процедур, которым необходимо следовать, а также на сроки ее принятия.

В плане разработки стратегии следует определить основные этапы и виды деятельности, ключевые заинтересованные стороны и потребности в ресурсах. В нем должно быть указано, как и на каком этапе соответствующие заинтересованные стороны могут принять участие в процессе разработки и представлять свои вклады и замечания.

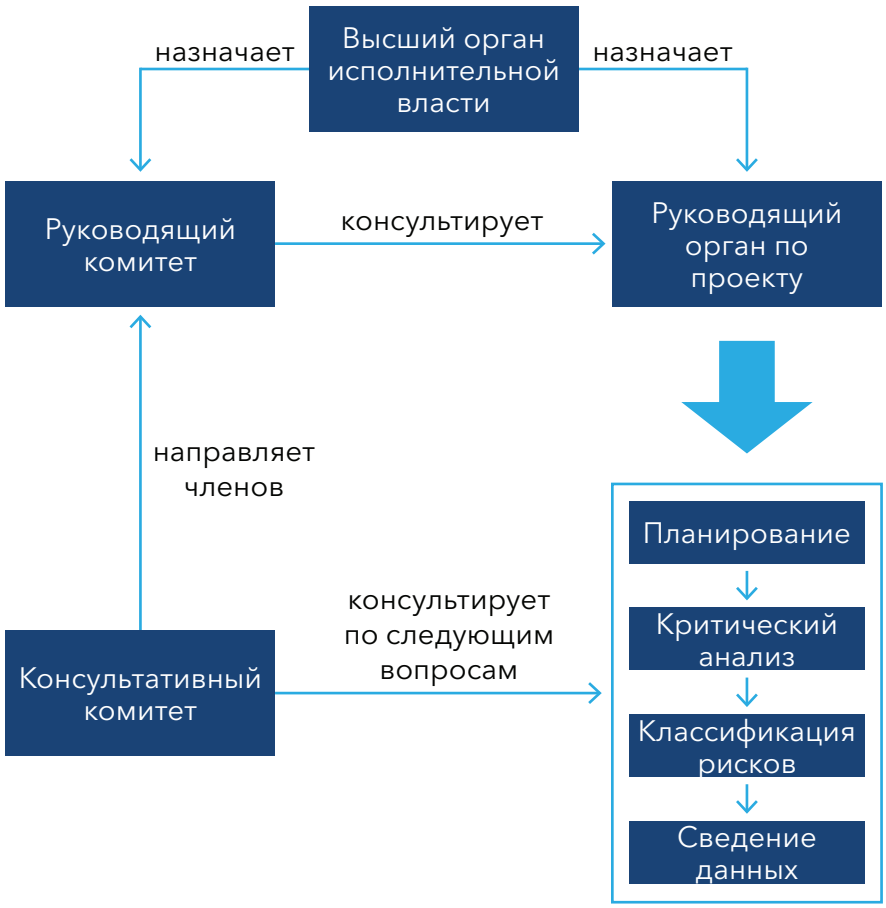
Следует также определить необходимые людские и финансовые ресурсы, а также их источники. Например, за необходимыми экспертными знаниями можно было бы обратиться к межправительственным организациям, частному сектору, академическим организациям или учреждениям, занимающимся вопросами развития. Аналогичным образом, потребности в финансировании можно было бы удовлетворить путем перераспределения целевых направлений финансирования в имеющихся бюджетах или путем привлечения нового финансирования от третьих сторон (например, международных организаций).

Особое внимание следует уделить обеспечению долгосрочного финансирования полного жизненного цикла национальной стратегии кибербезопасности, включая ее разработку, осуществление и уточнение. Дополнительная информация о распределении ресурсов на цели осуществления стратегии содержится в разделе под названием "Выделение людских и финансовых ресурсов на цели осуществления" (раздел 3.4.3), а о долгосрочном финансировании – в разделе "Выделение целевого бюджета и ресурсов" (раздел 5.1.5).

На Рисунке 2 показаны возможные линии взаимодействия и распределение функций между различными заинтересованными сторонами и комитетами.

Дополнительные справочные материалы перечислены на стр. 55.

***Рисунок 2** – Заинтересованные стороны*



3.2 Этап II: Обзор и критический анализ имеющегося опыта

Цель этого этапа заключается в сборе данных для оценки положения дел в стране в области кибербезопасности и текущих и будущих рисков, которая ляжет в основу подготовки и разработки национальной стратегии кибербезопасности. Результатом этой работы должен стать отчет с обзором стратегической национальной доктрины кибербезопасности и положения дел с рисками, который будет представлен руководящему комитету.

Прежде, чем приступить к практической разработке текста стратегии, руководящий орган по проекту должен провести тщательный анализ и оценку информации, собранной на этапе обзора имеющегося опыта, чтобы удостовериться в том, что все пробелы в механизмах обеспечения кибербезопасности были выявлены и представлены варианты их ликвидации. Результатом этого анализа должны стать оценка того, насколько существующая политическая, регуляторная и функциональная среда способствует достижению заявленных в стратегии целей, и выявление областей, в которых она не отвечает требованиям.

Аналогичным образом, этот анализ следует использовать для выявления конкретных ключевых проблем, таких как пробелы в образовании и подготовке.

Наконец, результатом анализа должна стать оценка всех значимых и желаемых конечных результатов стратегии, а также потенциального воздействия и результатов использования выбранных средств осуществления.

Дополнительные справочные материалы перечислены на стр. 55.

3.2.1 Оценка положения дел с кибербезопасностью в стране

Для того, чтобы национальная стратегия кибербезопасности была эффективной, в ней необходимо отразить доктрину кибербезопасности страны. В этих целях следует провести анализ существующих преимуществ и недостатков страны с точки зрения кибербезопасности, а также изучить материалы и документы по этой тематике в сотрудничестве с соответствующими заинтересованными сторонами, представляющими государственные органы, частный сектор и гражданское общество. На этом этапе следует применять принцип комплексного подхода и целевых приоритетов (описан в разделе 4.2).

В рамках этой деятельности руководящему органу по проекту следует определить активы и услуги, имеющие решающее значение для надлежащего функционирования общества и экономики, а также составить схему существующих национальных законов, норм, политики, программ и потенциала, касающихся кибербезопасности. Руководящий орган по проекту должен также определить существующие механизмы "мягкого" регулирования, такие как государственно-частные партнерства, и провести критический анализ технических возможностей, созданных для решения проблем в области кибербезопасности, например, национальных Групп реагирования на нарушения компьютерной защиты (CERT). Кроме того, следует определить функции и обязанности существующих государственных учреждений, занимающихся вопросами кибербезопасности, таких как регуляторные органы или учреждения по защите данных, и составить их схему.

Дополнительно следует собирать данные по этой тематике, которые могут лечь в основу доктрины кибербезопасности страны. Такие данные могут включать: информацию о существующих национальных программах в области кибербезопасности, международных инициативах, проектах частного сектора, учебных программах по ИКТ и кибернетике, а также программах развития навыков, киберинициативах в области НИОКР, данные об уровне проникновения интернета и его инфицирования, внедрении ИКТ, развитии технологий, а также аналитические материалы о будущих тенденциях и угрозах в области ИКТ и кибербезопасности.

В вышеупомянутый анализ следует также включить соответствующую информацию, предоставленную частным сектором, исследовательскими учреждениями и другими группами заинтересованных сторон. Для развивающихся стран решающее значение имеет также составление плана совместных инициатив по координации технической помощи и инвестиций с партнерами в области развития.

Наконец, руководящему органу по проекту следует также изучить аналогичную информацию на региональном и международном уровнях, а также рассмотреть конкретные стратегии и инициативы для каждого сектора.

3.2.2 Оценка положения дел в области киберрисков

Руководящему органу по проекту следует провести оценку рисков, с которыми сталкивается страна в связи с зависимостью от цифровых технологий, на основе собранной на предыдущем этапе информации. Такую оценку можно провести путем определения национальных цифровых активов, как государственных, так и частных, взаимосвязей между ними, факторов уязвимости и угроз, а также путем расчета вероятности возникновения киберинцидентов и их потенциального воздействия.

Эта деятельность выполняется в соответствии с принципом управления рисками и обеспечения устойчивости (раздел 4.6), в котором признается, что управление рисками имеет решающее значение для полномерного использования преимуществ цифровой среды в интересах социально-экономического развития. Кроме того, на основе этой первоначальной оценки рисков могут проводиться дальнейшие, более конкретные оценки рисков (более подробная информация о принципе оценки рисков и обеспечения устойчивости содержится в разделе 5.2).

3.3 Этап III: разработка национальной стратегии кибербезопасности

Цель этого этапа заключается в разработке текста стратегии с привлечением ключевых заинтересованных сторон из государственного и частного секторов, а также из гражданского общества в рамках серии общественных консультаций и рабочих групп. На этот более широкий круг заинтересованных сторон, координацию деятельности которых осуществляет руководящий орган по проекту, будет возложена задача определения общей концепции и сферы применения стратегии, постановки задач высокого уровня, анализа текущего положения дел (подробная информация содержится в описании этапа II), расстановки задач в порядке приоритетности с точки зрения воздействия на общество, граждан и экономику, а также обеспечения необходимых финансовых ресурсов. На этом этапе следует учитывать все сквозные принципы (раздел 4) и примеры передового опыта (раздел 5), подробно описанные в настоящем Руководстве.

3.3.1 Написание текста национальной стратегии кибербезопасности

По завершении этапа обзора и критического анализа имеющегося опыта руководящему органу по проекту в сотрудничестве с руководящим комитетом следует приступить к написанию стратегии. Могут создаваться специальные рабочие группы для рассмотрения конкретных тем или для написания различных разделов стратегии. Рабочие группы должны следовать установленным на этапе инициирования процедурам, корректируя их в случае необходимости.

В стратегии должны содержаться общие руководящие указания по кибербезопасности для страны; четкая концепция и сфера применения; задачи, которые следует решить в конкретные установленные сроки, а также порядок их приоритетности с точки зрения воздействия на общество, экономику и инфраструктуру. Кроме того, в ней следует определить возможные варианты порядка действий, стимулы для принятия мер по ее реализации, а также ориентиры для распределения ресурсов, требуемых для поддержки всех этих видов деятельности. В стратегию можно также включить некоторые выводы, сделанные по итогам этапа обзора и критического анализа имеющегося опыта.

По аналогии с этапом, на котором составляется план разработки стратегии, необходимо включить в данный документ четкую структуру управления (раздел 5.1), в которой определены функции и обязанности основных заинтересованных сторон. В этой структуре следует определить орган, ответственный за управление осуществлением стратегии и ее оценку, а также орган, ответственный за общее руководство и осуществление, например, один из центральных органов власти или национальный совет по кибербезопасности.

В стратегии также следует сформулировать или подтвердить мандаты различных структур, ответственных за представление предложений по политическим мерам и нормативным актам в области кибербезопасности страны и их разработку. Кроме того, в ней необходимо определить обязанности и задачи структур, ответственных за сбор информации по угрозам и факторам уязвимости, реагирование на киберинциденты (например, национальные CERT), повышение уровня готовности и осуществление управления в кризисных ситуациях.
В стратегии следует также четко прописать методы взаимодействия всех этих структур между собой и с центральным органом власти.

3.3.2 Консультации с широким кругом заинтересованных сторон

Как упоминалось выше, взаимодействие с заинтересованными сторонами имеет решающее значение для успешной разработки стратегии. Для того, чтобы убедиться, что заключительный текст стратегии основан на разделяемой всеми концепции, проект документа следует распространить среди широкого круга участников, не ограниченного теми, кто участвовал в процессе разработки стратегии. В этих целях можно предусмотреть различные формы взаимодействия, включающие онлайновые консультации, семинары-практикумы по утверждению текста и дополнительные рабочие группы. Предполагается, что полученные по итогам такого процесса замечания и комментарии будут использованы для доработки стратегии.

3.3.3 Процедура официального утверждения

На заключительной стадии разработки стратегии руководящий орган по проекту должен обеспечить официальное утверждение стратегии исполнительной властью. Такая процедура официального утверждения будет варьироваться от страны к стране, в зависимости от того, как определено место стратегии в законодательной базе. Например, она может быть утверждена в рамках парламентской процедуры или постановлением правительства.

Кроме того, важнейшее значение имеет не только утверждение разработанной стратегии на высшем уровне управления страной, но и сохранение этой приверженности на этапе ее осуществления. Соответствующие должностные лица должны представлять отчетность и располагать поддержкой в виде как политического капитала, так и ресурсов.

3.3.4 Публикация стратегии

Стратегия должна быть опубликована и доступна широкой общественности. Ее широкое распространение будет служить залогом осведомленности общественности о приоритетах и задачах правительства в области кибербезопасности, а также поддержки любых усилий, направленных на повышение осведомленности в вопросах кибербезопасности. Если стратегия будет сопровождаться планом действий, в нем также следует указать дополнительные возможности для дальнейшего взаимодействия и сотрудничества с гражданским обществом и частным сектором.

Дополнительные справочные материалы перечислены на стр. 55.

3.4 Этап IV: Осуществление

Этап осуществления является самым важным элементом общего жизненного цикла национальной стратегии кибербезопасности. Структурированный подход к осуществлению в сочетании с надлежащими людскими и финансовыми ресурсами имеет решающее значение для успешного осуществления стратегии, поэтому его следует учитывать при ее разработке. Основой этапа осуществления, как правило, становится план действий, в котором содержатся инструкции по реализации различных предусмотренных мер.

3.4.1 Разработка плана действий

Так же, как и в случае с разработкой стратегии, за ее осуществление не может отвечать лишь один орган власти. Напротив, эта деятельность требует взаимодействия и координации целого ряда различных заинтересованных сторон в разных государственных органах, а также поддержки со стороны гражданского общества и частного сектора. Поддержка эффективного осуществления стратегии может быть основана на плане действий, разработанном в соответствии с принципом четкого определения руководства, функций и распределения ресурсов (раздел 4.8).

Процесс разработки плана действий практически так же важен, как и план сам по себе. Этот процесс, координацию которого осуществляет руководящий орган по проекту, должен служить механизмом организации взаимодействия различных заинтересованных сторон для согласования задач и конечных результатов, а также для координации усилий и объединения ресурсов.

3.4.2 Определение инициатив, предназначенных для реализации

В национальной стратегии кибербезопасности описываются задачи правительства и конечные результаты, которые оно хочет получить в различных определенных в стратегии тематических областях. В плане действий руководящий орган по проекту должен определить в координации с соответствующими заинтересованными сторонами конкретные инициативы для каждой тематической области, которые помогут выполнить эти задачи. Примеры таких инициатив могут включать, среди прочего, организацию учений по кибербезопасности, введение базовых критериев безопасности для важнейшей инфраструктуры или создание системы сообщения об инцидентах.

Порядок приоритетности сроков реализации и мер, необходимых для осуществления таких инициатив, определяется в зависимости от степени их важности в интересах обеспечения надлежащего использования ограниченных ресурсов. В этих целях предлагается учитывать итоги и конечные результаты этапа II (обзор и критический анализ имеющегося опыта), касающиеся, в частности, оценки положения дел с киберрисками (раздел 3.2.2).

3.4.3 Выделение людских и финансовых ресурсов на цели осуществления

После выявления приоритетных инициатив руководящий орган по проекту должен определить конкретные государственные структуры, которые будут отвечать за осуществление каждой из них. Соответственно, эти государственные структуры будут отвечать за осуществление каждой конкретной инициативы и отчитываться по ней; предполагается, что в процессе осуществления они будут координировать свою деятельность с другими заинтересованными сторонами.

Для обеспечения того, чтобы эти структуры могли достигнуть ожидаемых результатов, руководящий орган по проекту должен провести оценку того, были ли им предоставлены соответствующие полномочия (правовые или иного характера), необходимые для осуществления стратегии. Руководящий орган по проекту должен также работать со структурами, ответственными за осуществление конкретных инициатив, с тем чтобы понимать, какие ресурсы необходимы для выполнения работы. Такая оценка должна охватывать людские ресурсы, потребности в специальном опыте и финансировании. После этого руководящему органу по проекту следует вести работу с ответственными структурами, с тем чтобы помочь им определить и найти необходимые ресурсы в соответствии с административной и финансовой структурой страны.

3.4.4 Определение графиков работы и разработка системы показателей

Заключительным важнейшим элементом плана действий является разработка специальных параметров и ключевых показателей деятельности для оценки каждой из осуществленных инициатив, например, проведение в стране кампании повышения осведомленности о важном значении обмена информацией; организация и проведение учений по кибербезопасности с представителями сектора важнейшей инфраструктуры; принятие в стране закона о базовых показателях безопасности. Следует также установить конкретный график осуществления.

Параметры и ключевые показатели деятельности должны разрабатываться руководящим органом по проекту в партнерстве с соответствующими ответственными структурами. Последним следует рекомендовать разработать и отслеживать более подробный набор показателей для упрощения оценки эффективности и результативности инициатив в ходе их выполнения и по его завершении.

Дополнительные справочные материалы перечислены на стр. 55.

3.5 Этап V: Мониторинг и оценка

На этом этапе компетентному органу следует разработать официальную процедуру мониторинга и оценки стратегии. На этапе мониторинга правительство должно обеспечить соответствие процесса осуществления стратегии ее плану действий. На этапе оценки правительство и его компетентный орган должны оценить, сохраняет ли стратегия свою актуальность с учетом изменяющегося положения дел с рисками, и отражает ли она задачи правительства, а также необходимость внесения корректировок.

3.5.1 Установление официальной процедуры

Для обеспечения эффективного мониторинга и оценки хода осуществления стратегии правительство должно будет определить независимый орган, на который будет возложена обязанность по мониторингу и оценке хода осуществления и эффективности. Было бы оптимально, если бы этот орган занимался определением необходимых параметров мониторинга и оценки хода осуществления стратегии и соответствующих плана действий и инициатив, которое должно осуществляться на этапах разработки и инициирования.

Мониторинг и измерение эффективности деятельности и прогресса в области выполнения плана осуществления стратегии должны стать частью механизмов управления, которые внедряет та или иная страна. Постоянная оценка хода выполнения плана осуществления (т. е. что продвигается успешно, а что нет) способствует учету в стратегии фактических данных. Механизмы надлежащего управления применительно к осуществлению стратегии должны также предусматривать четкое разграничение подотчетности и ответственности за успешное выполнение. Укреплению механизмов управления и руководства способствует определение параметров или ключевых показателей деятельности (KPI) для достижения целей на краткосрочную, среднесрочную и долгосрочную перспективу. Ключевые показатели деятельности или параметры должны быть:

- ***конкретными***: следует определить конкретную область, в которой необходимы усовершенствования;
- ***измеримыми***: следует задать или по крайней мере наметить количественный показатель хода осуществления;
- ***осуществимыми***: следует установить, какие результаты могут быть реально достигнуты с учетом имеющихся ресурсов;
- ***определяющими ответственного исполнителя***: следует определить, кому поручить эту работу;
- ***учитывающими время***: следует определить, когда может (могут) быть достигнут(ы) результат(ы).

Определение базовых параметров позволит лучше отслеживать действия и выявлять области, которые могут потребовать улучшения. Кроме того, распределение бюджетных средств должно осуществляться сообразно масштабности и сложности желаемого воздействия.

3.5.2 Мониторинг прогресса в осуществлении стратегии

Орган, на который возлагается обязанность по мониторингу прогресса в осуществлении стратегии, должен осуществлять этот мониторинг, ориентируясь на согласованные сроки на всем протяжении жизненного цикла стратегии. В итоговом документе о таком мониторинге (например, отчете) должны быть отражены любые отклонения от согласованных сроков и причины любых задержек, например смещение приоритетов, дефицит кадров или других ресурсов и т. д. Эта деятельность дополняет регулярное представление руководящему органу по проекту новой информации структурами, ответственными за различные направления деятельности по осуществлению стратегии.

Такой подход позволит обеспечить подотчетность соответствующих заинтересованных сторон с точки зрения выполнения возложенных на них обязательств; он также позволит выявлять любые трудности в процессе осуществления стратегии на ранних этапах. Это, в свою очередь, даст правительствам возможность либо исправить ситуацию, либо соответствующим образом адаптировать свои планы с учетом уроков, извлеченных в процессе осуществления.

3.5.3 Оценка результатов стратегии

Помимо оценки прогресса с использованием согласованных параметров, также важно периодически оценивать результаты, сопоставляя их с поставленными задачами. Это крайне важно для понимания того, выполняются ли задачи стратегии или же необходимо рассмотреть возможность принятия различных мер. В рамках этого процесса необходимо также проводить повторные оценки более широкого контекста с точки зрения рисков, для того чтобы понять, оказывают ли воздействие на результаты стратегии какие-то внешние изменения. По сути этот процесс представляет собой облегченную процедуру пересмотра профиля характерных для страны рисков.

Оценка наряду с соответствующими рекомендациями должна быть включена в отчет для руководящего органа по проекту и содержать сведения о способах обновления плана действий, а также обеспечения его актуальности и учета в нем политических изменений и структуры рисков.

В конечном итоге отчеты, подготавливаемые на всем протяжении жизненного цикла стратегии, должны также лечь в основу общего процесса пересмотра национальной стратегии в области кибербезопасности в соответствии со сроками, установленными на этапе инициирования. В процессе такого всеобъемлющего пересмотра должен рассматриваться не только достигнутый прогресс и изменения внешних условий, в нем должна также содержаться проведенная переоценка приоритетов и задач правительства.

Дополнительные справочные материалы перечислены на стр. 55.

4 Всеобъемлющие принципы

В данном разделе представлены девять сквозных принципов, которые в совокупности могут служить подспорьем в разработке ориентированной на будущее целостной национальной стратегии в области кибербезопасности.

Эти принципы могут применяться ко всем ключевым тематическим областям, определенным в настоящем документе. Их следует учитывать на всех этапах процесса разработки национальной стратегии, от составления проекта текста национальной стратегии и вплоть до ее осуществления.

Принципы излагаются в логической последовательности, а не по степени важности.

4.1 Концепция

В настоящей стратегии должна излагаться четкая концепция, учитывающая мнения государства и общества во всей их полноте.

Более весомые шансы на успех имеет стратегия, в которой излагается концепция, позволяющая всем заинтересованным сторонам осознать, какова значимость этого вопроса и почему стратегия является необходимой (контекст), чего нужно добиться (задачи), а также в чем она состоит и какое воздействие она окажет (сфера действия).

Чем отчетливее изложена концепция, тем легче будет руководителям и ключевым заинтересованным сторонам обеспечить более комплексный, последовательный и целостный подход. Четкая концепция также позволяет достичь лучшей координации действий различных заинтересованных сторон, более полного их сотрудничества и лучшего осуществления стратегии. Она должна быть сформулирована на достаточно высоком уровне, с учетом динамичного характера цифровой среды.

Задачи и сроки осуществления стратегии должны соотноситься с этой концепцией.

Дополнительные справочные материалы перечислены на стр. 56.

4.2 Всеобъемлющий подход и ориентированные на конкретные особенности приоритеты

Стратегия должна основываться на всеобъемлющем понимании и анализе общей цифровой среды, однако при этом учитывать особые обстоятельства страны и включать классификацию приоритетов.

Кибербезопасность представляет собой не просто техническую проблему, а комплексный многогранный вопрос, различные аспекты которого затрагивают не только экономическое и социальное процветание, но и другие области, такие как правоприменение, национальная и международная безопасность, международные отношения, торговые переговоры, устойчивое развитие и др.

Большое значение имеет понимание всех аспектов кибербезопасности и того, каким образом они взаимосвязаны, могут ли они быть взаимодополняющими или конкурирующими. На основании этого понимания и анализа конкретной ситуации в стране можно определить приоритеты, соответствующие задачам и срокам осуществления стратегии. Наличие приоритетов позволит определить конкретные задачи и сроки и распределить необходимые ресурсы.

Перечень приоритетов, включаемых в национальную стратегию в области кибербезопасности, будет варьироваться в зависимости от страны. Некоторые из тем, связанных с кибербезопасностью, могут рассматриваться в одном и том же или в отдельных стратегических документах (так, например, цифровые аспекты национальной безопасности и обороны могут рассматриваться в национальной стратегии в области безопасности либо в области обороны).

Дополнительные справочные материалы перечислены на стр. 56.

4.3 Открытость для всех

Стратегия должна разрабатываться при активном участии всех соответствующих заинтересованных сторон и учитывать их потребности и обязательства.

Цифровая среда приобрела важнейшее значение для правительства, делового сообщества и отдельных лиц. Эти группы сталкиваются с рисками в области кибербезопасности и, в зависимости от своей роли, несут определенную меру ответственности за управление этими рисками. Непременным условием разработки и успешного осуществления национальной стратегии в области кибербезопасности являются определение и привлечение к этому процессу всех соответствующих заинтересованных сторон, какой бы сложной задачей это ни было. Эти меры помогут понять потребности заинтересованных сторон и ознакомиться с их уникальными знаниями и экспертным опытом, поощряя тем самым сотрудничество в целях выполнения задач стратегии.

В целях обеспечения принципа открытости для всех следует сделать стратегию общедоступным документом.

Дополнительные справочные материалы перечислены на стр. 56 и 57.

4.4 Экономическое и социальное процветание

Стратегия должна способствовать экономическому и социальному процветанию и максимальному увеличению вклада ИКТ в устойчивое развитие и социальную интеграцию.

Цифровая среда обладает потенциалом по ускорению экономического роста и социального прогресса, поощрению ключевых социальных ценностей, усовершенствованию системы оказания государственных услуг и укреплению ее потенциала, содействию международной торговле и надлежащему управлению.

Все более широкое использование цифровой среды для удовлетворения запросов общества требует повышенного внимания к вопросам кибербезопасности. В то же время кибербезопасность не является самоцелью; необходимо обеспечить согласование стратегии с более широкими социально-экономическими задачами, а также ее нацеленность на укрепление доверия и уверенности, необходимых как для реализации этих задач, так и для защиты страны от киберугроз.

Дополнительные справочные материалы перечислены на стр. 57.

4.5 Основополагающие права человека

Стратегия должна предусматривать уважение основополагающих ценностей и согласовываться с ними.

В стратегии должен признаваться тот факт, что права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде. В стратегии должно обеспечиваться уважение общепринятых основополагающих прав, включая, среди прочего, права, изложенные во Всеобщей декларации прав человека и Международном пакте о гражданских и политических правах Организации Объединенных Наций, а также в соответствующих многосторонних и региональных нормативно-правовых системах.

Необходимо уделять внимание свободе выражения мнений, конфиденциальности сообщений и защите личных данных. В частности, в стратегии не должна поощряться практика произвольного, необоснованного и другого незаконного слежения за сообщениями, их перехвата или обработки персональных данных.

Стратегия, призванная обеспечивать сбалансированное соблюдение потребностей государства и отдельных граждан, должна гарантировать, что, когда это применимо, слежение за сообщениями, их перехват или сбор данных будут осуществляться в рамках конкретного расследования или судебного дела, на основании разрешения соответствующего национального органа и в соответствии с общедоступными, четкими, всеобъемлющими и недискриминационными правовыми нормами, обеспечивающими возможность эффективного надзора, процессуальные гарантии и средства правовой защиты.

Дополнительные справочные материалы перечислены на стр. 57 и 58.

4.6 Управление рисками и устойчивость

Стратегия должна предусматривать возможность эффективного управления рисками в области кибербезопасности и способствовать повышению устойчивости экономической и социальной деятельности.

Цифровая среда, создающая экономические и социальные возможности для заинтересованных сторон, одновременно подвергает их риску в области кибербезопасности. Например, в случаях, когда организации используют ИКТ для поощрения инноваций, повышения производительности и конкурентоспособности, или когда правительства предоставляют онлайновый доступ к своим услугам, могут иметь место связанные с кибербезопасностью инциденты, что чревато финансовыми потерями, ущербом для репутации, функциональными сбоями, препятствиями инновационному развитию и т. д. Как и другие виды рисков, риски в области кибербезопасности нельзя полностью устранить, однако их можно регулировать и минимизировать.

В целях решения этой проблемы стратегия должна побуждать организации уделять приоритетное внимание вопросу инвестирования в кибербезопасность и разработке профилактических мер по управлению рисками. В зависимости от степени готовности организации к принятию рисков, ей следует поддерживать баланс между мерами по обеспечению безопасности и потенциальной выгодой, с учетом динамичного характера цифровой среды. Кроме того, в стратегии должна признаваться необходимость непрерывного процесса управления рисками, а также должно поощряться применение целостного подхода в отношении ряда взаимозависимых организаций.

Особое внимание к вопросам управления рисками также будет способствовать повышению готовности заинтересованных сторон к потенциальным инцидентам, связанным с кибербезопасностью, обеспечению устойчивости экономической и социальной деятельности в стране. С учетом этого стратегия должна поощрять принятие мер по обеспечению непрерывности деловой активности, предполагающих управление инцидентами и рисками, а также планов по восстановлению.

Дополнительные справочные материалы перечислены на стр. 58.

4.7 Надлежащий набор политических инструментов

Стратегия должна предполагать применение наиболее подходящих из имеющихся в распоряжении политических инструментов для выполнения каждой из определенных в ней задач, с учетом конкретных обстоятельств страны.

Цели правительства в области кибербезопасности могут быть достигнуты только при условии, что изменится поведение всех заинтересованных сторон процесса. В большинстве случаев в распоряжении правительств имеются различные рычаги и политические инструменты, позволяющие этого добиться. К ним относятся законодательство, регулирование, стандартизация, программы и механизмы стимулирования и обмена информацией, образовательные программы, обмен передовым опытом, определение ожидаемых норм поведения, а также, среди прочего, построение сообществ, основанных на доверии. Все эти меры имеют свои преимущества и недостатки, требуют разных затрат и позволяют достичь разных результатов.

Наилучших результатов можно добиться путем определения наиболее подходящего политического инструмента для выполнения каждой конкретной задачи и сбалансированного использования различных средств.

Дополнительные справочные материалы перечислены на стр. 59.

4.8 Четкое определение руководства, функций и распределение ресурсов

Следует утвердить стратегию на самом высоком уровне правительства, которое в таком случае будет отвечать за распределение соответствующих функций и обязанностей и выделение достаточных людских и финансовых ресурсов.

Кибербезопасность должна поощряться и пользоваться поддержкой на самом высоком правительственном уровне. Кроме того, в целях обеспечения подотчетности и прогресса необходимо определить координаторов по отдельным направлениям работы, при этом все участвующие стороны должны иметь четкое представление о собственных функциях и обязанностях.

В стратегии также должно быть предусмотрено выделение людских, финансовых и материальных ресурсов, необходимых для ее осуществления. Этим принципом необходимо руководствоваться как в процессе разработки стратегии, так и при подготовке соответствующего плана действий.

Дополнительные справочные материалы перечислены на стр. 59.

4.9 Доверительная среда

Стратегия должна способствовать созданию цифровой среды, заслуживающей доверия граждан и делового сообщества.

Создание и укрепление доверительных отношений в национальной цифровой экосистеме, в которой защищаются права и интересы пользователей и обеспечивается безопасность данных и систем, имеет важнейшее значение для полноценного раскрытия потенциала в социальной, политической и экономической областях, создаваемого благодаря использованию ИКТ. Стратегия должна обеспечить возможность применения на национальном уровне политики, процедур и мер, гарантирующих предоставление жизненно необходимых услуг (включая электронное правительство, электронную торговлю, цифровые финансовые операции и др.) при помощи ИКТ и их использование гражданами. Такой порядок действий будет способствовать укреплению принципа доверия не только среди населения в целом, но и в тех государственных и частных организациях, которые будут предоставлять гражданам свои услуги, связанные с ИКТ.

Дополнительные справочные материалы перечислены на стр. 59.

5 Передовая практика, касающаяся национальной стратегии в области кибербезопасности

Ситуация в сфере кибербезопасности влияет на многие области социально-экономического развития и подвергается воздействию со стороны ряда факторов в национальном контексте.

В связи с этим в настоящем разделе описывается комплекс примеров передового опыта, которые позволят обеспечить всеобъемлющий характер и эффективность стратегии при должном учете конкретных национальных условий.

Эти примеры передового опыта объединены в отдельные тематические области, которые представляют собой всеобъемлющие темы для учета в национальной стратегии кибербезопасности. В качестве примеров передового опыта здесь приводятся как тематические области, так и отдельные элементы, однако весьма важно отметить, что последние следует рассматривать в национальном контексте, поскольку некоторые из них могут быть неактуальны для какой-либо конкретной страны. Странам следует определить и применять те примеры передового опыта, которые способствуют реализации их собственных задач и приоритетов в соответствии с концепцией, изложенной в их стратегии (раздел 4). Порядок, в котором ниже приводятся отдельные элементы или тематические области, никак не указывает на их степень важности или приоритетности.

5.1 Тематическая область 1 – Управление

В данной тематической области приводятся элементы передового опыта, которые следует рассматривать с точки зрения возможности включения в раздел стратегии, в котором описывается структура управления в области национальной кибербезопасности. В стратегии должны быть четко изложены задачи и ожидания в сфере кибербезопасности, которыми руководствуется правительство, а также определены функции и порядок подотчетности, необходимые для ее осуществления.

Для этих целей в рамках стратегии следует определить компетентный орган, который отчитывается за осуществление стратегии, и наделить его соответствующими полномочиями; создать механизм для определения и обеспечения участия государственных структур, затрагиваемых осуществлением стратегии или ответственных за ее реализацию; закрепить в плане по осуществлению стратегии конкретные, измеримые, выполнимые, ориентированные на конкретные результаты и сроки задачи и признать необходимость выделения ресурсов (например, политической воли, финансирования, времени и людских ресурсов) для достижения желаемых результатов.

5.1.1 Обеспечение поддержки на самом высоком уровне

Стратегия должна быть официально одобрена на самом высоком правительственном уровне. Такое одобрение служит двум важным целям. Во-первых, оно повышает вероятность выделения достаточных ресурсов и успешной координации действий. Во-вторых, оно показывает более широкой национальной экосистеме, что обеспечение кибербезопасности имеет для страны важное значение.

5.1.2 Создание компетентного органа по вопросам кибербезопасности

В стратегии следует определить специализированный национальный орган по вопросам кибербезопасности – руководящий орган (конкретное лицо или организацию), обладающий весомым положением и большим влиянием на самом высоком правительственном уровне, который будет обеспечивать руководство, координацию действий и мониторинг хода осуществления стратегии.

Такой национальный компетентный орган по вопросам кибербезопасности должен также играть роль управляющей структуры в том, что касается определения и уточнения функций, обязанностей, процедур, прав на принятие решений, а также задач, необходимых для обеспечения эффективного осуществления стратегии. Это подразумевает определение заинтересованных сторон, которые будут следить за ходом осуществления стратегии, и установление целевых показателей эффективности деятельности для различных министерских и правительственных структур, учреждений или лиц, ответственных за конкретные аспекты стратегии и последующего плана действий. Такой подход может потребовать создания дополнительных политических или правовых структур, для того чтобы наделить эти заинтересованные стороны полномочиями в целях осуществления их миссии.

С учетом того факта, что кибербезопасность является общей задачей для различных областей вопросов, важно обеспечить способность национального компетентного органа привлекать к участию и направлять соответствующие заинтересованные стороны.

5.1.3 Обеспечение внутриправительственного сотрудничества

Стратегия должна предусматривать создание механизма в целях определения и обеспечения участия государственных структур, имеющих отношение к ее осуществлению либо ответственных за него. Основными функциями этих государственных структур являются целеустремленная работа, координация действий и сотрудничество внутри правительства, необходимые для того, чтобы при помощи механизмов управления (то есть правил) и выделяемых ресурсов обеспечить достижение желаемых результатов стратегии.

Эффективная связь и координация действий способствуют тому, что все министерства и государственные ведомства располагают сведениями о соответствующих полномочиях, задачах и поручениях друг друга. Тем не менее целеустремленная работа предполагает постоянную поддержку последовательной политики для того, чтобы обеспечить выполнение обязательств, закрепленных в рамках стратегии. В качестве примера координационного механизма можно привести периодическое проведение собраний для совместного обзора планов действий при участии всех соответствующих заинтересованных сторон. Примером механизма сотрудничества может служить создание внутриправительственной целевой группы по урегулированию определенного вопроса. Примером целеустремленной работы является обеспечение согласованности внутриполитической и внешнеполитической программ страны, с тем чтобы действия одного министерства не подрывали доверие к другому министерству по причине представления различных позиций по одной и той же политической проблематике.

5.1.4 Обеспечение межсекторального сотрудничества

В стратегии должно быть отражено понимание существующей взаимозависимости в вопросах обеспечения кибербезопасности между правительством с одной стороны и частным сектором и другими национальными заинтересованными сторонами, с другой. В этих целях в стратегии должно быть изложено, каким образом правительство будет привлекать к участию эти заинтересованные стороны и определять их функции и обязанности. Например, в рамках стратегии следует определить сеть авторитетных национальных координаторов для ключевых отраслей, которые незаменимы для функционирования и восстановления важнейших услуг и инфраструктуры.

5.1.5 Выделение специального бюджета и ресурсов

Стратегия должна предусматривать выделение специальных и достаточных ресурсов для ее осуществления, поддержания и пересмотра. Достаточное, последовательное и непрерывное финансирование является основой уверенной национальной позиции в вопросах обеспечения кибербезопасности. Следует определить такие ресурсы, как денежные (специальный бюджет), людские, материальные, а также взаимодействие, партнерские связи и постоянная политическая приверженность и руководство, необходимые для успешной

реализации. Выделение ресурсов для выполнения задач и поручений в рамках стратегии не должно рассматриваться как разовое мероприятие. Ресурсы могут выделяться на конкретные задачи и поручения либо конкретным государственным структурам.

Правительство также может рассмотреть возможность формирования централизованного бюджета для целей кибербезопасности, управление которым будет осуществлять центральный исполнительный механизм в области кибербезопасности. Независимо от того, будут ли разрозненные источники финансирования объединяться в рамках согласованной комплексной программы или же будет создан единый внутриправительственный бюджет, для успешного осуществления стратегии необходимо обеспечить управление общей программой и поэтапное отслеживание хода ее реализации.

5.1.6 Разработка плана осуществления

Стратегия должна сопровождаться планом осуществления, в котором более подробно описывается, как будут выполняться ее стратегические задачи, или содержать ссылку на такой план. В эффективных планах осуществления указываются подотчетная структура, ответственная за выполнение каждого поручения и задачи; ресурсы, необходимые для их выполнения в течение определенного периода времени (краткосрочного, среднесрочного или долгосрочного); процедуры, которые будут применяться, и ожидаемые результаты (раздел 3.4, касающийся начального этапа осуществления).

Дополнительные справочные материалы перечислены на стр. 60 и 61.

5.2 Тематическая область 2 – Управление рисками в области национальной кибербезопасности

В данной тематической области представлен передовой опыт решения вопросов, связанных с кибербезопасностью, при помощи управления рисками. Как предусматривает принцип управления рисками и устойчивости (раздел 4.2), необходимо разработать подход к управлению рисками, поскольку полное устранение киберрисков не представляется возможным. Напротив, принятие мер к тому, чтобы страны хорошо осознавали те риски, которым они подвергаются, позволит им наиболее эффективным образом управлять этими рисками. В том, что касается оценки рисков, данный подход должен быть направлен прежде всего на выявление существующей взаимозависимости, а также учитывать риски, возникающие в связи с трансграничной зависимостью. В подходе к управлению рисками должен охватываться весь жизненный цикл, от разработки и закупок до функционирования и замещения.

Также важно отметить, что ввиду чрезвычайной динамичности и непредсказуемости киберугроз подход к управлению рисками, следует регулярно пересматривать. В самой стратегии должен содержаться план по мониторингу и оценке деятельности по управлению рисками в целях обеспечения постоянного улучшения.

5.2.1 Определение подхода к управлению рисками

В стратегии должен быть сформулирован согласованный подход к управлению рисками, которого будут придерживаться все государственные структуры и операторы важнейшей инфраструктуры, определяемые на национальном уровне. С помощью этого подхода следует определить ключевые ресурсы и услуги, необходимые для надлежащего функционирования общества и экономики, а также связанные с ними угрозы и риски.

Этот подход должен быть направлен на разработку национального реестра рисков при обеспечении условий безопасного хранения и передачи данных, для того чтобы создать возможности для осуществления правительственного надзора за рисками и подходами к управлению ими. Кроме того, в рамках подхода должен быть сформирован метод расстановки приоритетов на основе подсчета вероятности оцениваемых рисков и их последствий. Помимо этого, в нем должны быть изложены обязанности ключевых структур в каждом секторе в отношении оценки, принятия и преодоления рисков в области кибербезопасности на национальном уровне.

5.2.2 Определение общей методологии управления рисками в области кибербезопасности

В стратегии должна быть определена общая методология управления рисками в области кибербезопасности. Это позволит обеспечить эффективность и последовательность действий всех организаций и облегчит процесс обмена информацией о рисках между взаимозависимыми системами. Предпочтительно разработать методологию, основанную на международных стандартах, поскольку это позволит снизить издержки и обеспечить более эффективное взаимодействие с частным сектором.

В этой методологии должны содержаться руководящие указания по вопросам распределения функций и обязанностей в различных аспектах деятельности по управлению рисками, таких как оценка угроз, активов, принятие и поддержание мер по смягчению воздействия и принятие остаточного риска. Методология должна предусматривать программу сертификации, способствующую оценке и в конечном счете повышению уровня соответствия.

Важно отметить, что в том, что касается закупок и развития инфраструктуры или услуг, методология управления рисками должна также содержать руководящие указания по минимизации рисков при помощи безопасной архитектуры и проектирования, при том понимании что безопасность легче всего обеспечить, если она является неотъемлемой составляющей процесса проектирования продукта, процесса или услуги (*проектируемая безопасность*).

5.2.3 Составление профилей рисков секторов в области кибербезопасности

Стратегия должна поощрять использование профилей рисков секторов в области кибербезопасности. Профиль рисков сектора представляет собой количественный анализ видов существующих угроз. Целью составления профиля рисков является обеспечение более объективного представления о рисках путем присвоения цифровых значений переменным, представляющим различные виды угроз и той опасности, которую они представляют. В стратегии должно рекомендоваться составление профилей рисков для тех секторов, которые страна считает важнейшими для своего общества и экономики.

Использование профилей рисков секторов создает основу для более конкретных оценок рисков для отдельных организаций, обеспечивает согласованность внутри секторов и между всеми секторами на национальном уровне и позволяет сократить объем ресурсов, необходимых для проведения оценки организационных рисков. Профили рисков должны регулярно обновляться с целью поддержания их актуального характера.

5.2.4 Формирование политики в области кибербезопасности

Стратегия должна поощрять формирование политики в области безопасности для ключевых национальных структур, в частности таких, как государственные органы власти и операторы важнейшей инфраструктуры. Такая политика, которая будет принята в соответствии с принципом надлежащего набора политических инструментов (раздел 4.7), будет охватывать вопросы управления, эксплуатационных и технических требований, содержать для заинтересованных сторон инструкции относительно их функций и обязанностей, а также руководящие указания и поручения относительно конкретных подходов к этим вопросам.

Например, это может быть политика, направленная на обеспечение кибербезопасности в сфере закупок или разработки, определение программ по обмену информацией, координацию в вопросах раскрытия информации об уязвимости, установление минимальных стандартов обслуживания, определение базовых уровней безопасности и программ сертификации соответствия, а также политика, содержащая поручения относительно представления отчетов о киберинцидентах.

Применение скоординированного подхода на национальном уровне позволит добиться более эффективного и результативного управления в области кибербезопасности, поскольку это будет способствовать согласованию практических методов, улучшению координации и функциональной совместимости.

Дополнительные справочные материалы перечислены на стр. 61.

5.3 Тематическая область 3 – Обеспечение готовности и устойчивости

В данной тематической области приводится общий обзор передового опыта содействия созданию и устойчивому использованию действенного национального потенциала по предотвращению и обнаружению крупных инцидентов в области кибербезопасности, смягчению их последствий и реагированию на них, а также по повышению общей киберустойчивости страны.

5.3.1 Создание потенциала реагирования на киберинциденты

Стратегия должна поощрять создание соответствующего национального потенциала в области реагирования на инциденты в целях преодоления оперативных проблем, связанных с кибербезопасностью. Нередко создание такого потенциала предполагает учреждение групп реагирования на нарушение компьютерной защиты (CERT), групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT) и групп реагирования на компьютерные инциденты (CIRT), с полномочиями национального уровня.

Хотя конкретная форма организации CERT/CSIRT/CIRT может варьироваться (например, национальная, правительственная, секторальная и т. д.), а страны могут иметь разные потребности и ресурсы, эти специализированные целевые группы должны выполнять набор функций по предупреждению и реагированию, а также оказывать услуги в области предотвращения и обучения. Таким образом, эти структуры способны укрепить возможности страны по оперативному реагированию на кибератаки и восстановлению после них, а также повысить ее устойчивость перед киберугрозами, способствуя тем самым сокращению потенциальных общих экономических и оперативных последствий кибератак национального масштаба.

В рамках стратегии также должны быть определены и разработаны механизмы сотрудничества и процедуры связи между национальными и секторальными группами реагирования на инциденты (в том случае, если таковые имеются в стране), а также связи с зарубежными партнерами.

5.3.2 Создание планов действий на случай непредвиденных ситуаций в целях кризисного регулирования в области кибербезопасности

Стратегия должна поощрять разработку национального плана действий на случай непредвиденных ситуаций в целях реагирования на чрезвычайные ситуации и кризисы в области кибербезопасности. Такой план должен быть частью общего национального плана действий на случай непредвиденных ситуаций или согласовываться с ним. Следует также рассмотреть возможность разработки специального плана для важнейшей информационной инфраструктуры.

В этом национальном плане действий на случай непредвиденных ситуаций в области кибербезопасности должны учитываться результаты национальных оценок рисков и любая существующая межсекторальная зависимость, способная повлиять на непрерывность функционирования важнейшей инфраструктуры, а также любые механизмы восстановления после бедствий. Кроме того, в нем должен содержаться общий обзор национальных механизмов реагирования на инциденты, а также описание того, как осуществляется классификация инцидентов в области кибербезопасности с учетом их последствий для важнейших активов и услуг.

5.3.3 Содействие обмену информацией

Стратегия должна поощрять учреждение механизмов обмена информацией, которые позволят осуществлять обмен имеющими практическую направленность разведданными и информацией об угрозах между государственным и частным секторами.

Программы официального и неофициального обмена информацией могут служить подспорьем эффективной координации действий и обеспечению последовательной, точной и надлежащей связи в процессе реагирования на инциденты и восстановления; быстрому обмену информацией об угрозах и разведывательной информацией между сторонами, затронутыми инцидентом, и другими заинтересованными сторонами; более полному пониманию того, как и на какие сектора была осуществлена атака; распространению информации о методах, которые могут применяться в целях защиты пострадавших активов и минимизации нанесенного им ущерба, и в конечном счете сокращению факторов уязвимости и незащищенности, а также сопутствующих им рисков.

В стратегии должны быть определены одна или несколько институциональных структур (то есть компетентных органов), которые отвечают за передачу точной, имеющей практическую направленность информации всему национальному сообществу, занимающемуся вопросами кибербезопасности, включая государственный и частный секторы.

Обмен информации должен представлять собой двусторонний процесс. Если правительство готово делиться информацией, которая находится в его распоряжении, своими действиями оно сможет продемонстрировать структурам частного сектора, что действительно является партнером в процессе обмена информацией об угрозах, и будет способствовать принятию мер к тому, чтобы службы реагирования уделяли приоритетное внимание реагированию на ключевые угрозы и были лучше к нему подготовлены.

5.3.4 Проведение учений по кибербезопасности

В стратегии должны поощряться организация и координация национальных и международных учений по кибербезопасности и реагированию на инциденты. Они могут предполагать различные форматы (например, моделирование или учения в реальном времени) и быть ориентированы на техническую аудиторию или лиц, ответственных за принятие решений.

Учения по кибербезопасности и другие механизмы кризисного планирования могут помочь странам в развитии институционального потенциала для эффективного реагирования на инциденты, тестировании процедур кризисного управления и механизмов связи, проверке функциональных возможностей CERT/CSIRT/CIRT по оперативному реагированию и выявлении существующей межсекторальной зависимости.

Аналогичным образом, международные учения по кибербезопасности могут помочь государствам в укреплении потенциала по реагированию на киберинциденты, выявлении трансграничной зависимости, укреплении взаимного доверия и уверенности между странами и повышении общей способности к восстановлению и готовности на международном уровне.

Дополнительные справочные материалы перечислены на стр. 62 и 63.

5.4 Тематическая область 4 – Услуги важнейшей инфраструктуры и необходимые услуги

В настоящей тематической области исследуется передовой опыт защиты важнейшей инфраструктуры (CI) и, в частности, важнейшей информационной инфраструктуры (CII). Хотя общепризнанных определений этих двух терминов не существует и правительствам необходимо самим решать вопрос о том, какие структуры и услуги следует включить в это понятие на основании результатов национальной оценки рисков, для целей настоящего Руководства эти термины определяются следующим образом:

- *Важнейшая инфраструктура* (CI) – термин, используемый для описания активов, которые необходимы для функционирования и обеспечения безопасности общества и экономики в каждой конкретной стране;
- *Важнейшая информационная инфраструктура* (CII) – это системы ИТ и ИКТ, обеспечивающие управление ключевыми функциями важнейшей инфраструктуры страны.

В качестве альтернативы может использоваться понятие необходимых услуг, означающее услуги, которые являются необходимыми для поддержания важнейшей социальной или экономической деятельности.

Применительно к любому из этих случаев можно привести, помимо прочего, следующие примеры таких услуг: энергетика (электричество, нефть и газ), транспорт (воздушный, железнодорожный, водный и автомобильный), финансовая и банковская деятельность (кредитные учреждения, торговые площадки и центральные контрагенты), здравоохранение (организации здравоохранения, в том числе больницы и частные клиники), снабжение питьевой водой и ее распределение, цифровая связь и электросвязь (например, услуги фиксированной и подвижной телефонной связи и обеспечение инфраструктуры интернета, например пунктов обмена трафиком интернета (IXP), услуг наименования доменов).

5.4.1 Внедрение подхода к управлению рисками для защиты важнейшей инфраструктуры и услуг

Стратегия должна предусматривать защиту CI и CII с точки зрения управления рисками, в соответствии с принципом управления рисками и устойчивости (раздел 4.6). При определении национальной CI и CII и важнейших услуг, нарушение в работе которых может иметь серьезные последствия для здоровья, безопасности, охраны или экономического благосостояния граждан либо для эффективного функционирования правительства или экономики, следует руководствоваться результатами тщательной оценки рисков.

Кроме того, подход к управлению рисками должен также применяться в процессе определения и классификации в порядке приоритетности осуществляемых программ и политики, призванных обеспечивать защиту CI и CII. В целях содействия привлечению частного сектора может быть также рассмотрена возможность использования подхода к управлению рисками, разработанного на основе международных стандартов.

5.4.2 Внедрение модели управления, предусматривающей четкие обязанности

Стратегия должна содержать общее описание структуры управления, функций и обязанностей различных заинтересованных сторон, участвующих в защите CI и CII. Как предусматривает принцип четкого определения руководства, функций и распределения ресурсов (раздел 4.8), эффективная и результативная программа защиты CI требует от заинтересованных сторон выполнения четко определенных функций и обязанностей и создания координационного механизма для урегулирования текущих вопросов.

CI и CII нередко являются собственностью или находятся под контролем неправительственных субъектов, и возможностей и полномочий какой-то одной структуры правительства обычно недостаточно для того, чтобы обеспечить защиту CI и CII. Поэтому значительным подспорьем в усилиях по защите важнейшей инфраструктуры может стать назначение общего координатора по вопросам (кибер-)безопасности CI и CII, например межведомственного комитета.

Модель управления в области защиты CI и CII должна предусматривать определение государственных структур, ответственных за конкретные направления, обязанностей и подотчетности операторов CI и CII, а также каналов связи и механизмов сотрудничества между государственными и частными ведомствами в целях обеспечения функционирования и восстановления важнейших услуг и инфраструктуры.

5.4.3 Определение минимальных базовых уровней кибербезопасности

В стратегии должны быть указаны существующие либо предложены новые законодательные и нормативные рамки, в которых будут обозначены минимальные базовые уровни кибербезопасности, в частности для операторов CI и CII. При разработке таких уровней следует принимать во внимание признанные на международном уровне стандарты и передовую практику в целях обеспечения лучших результатов с точки зрения безопасности и большей эффективности.

Базовые уровни безопасности должны быть ориентированными на конкретные результаты, при этом следует четко определить, каких целей необходимо достичь организациям (например, "обеспечить контроль логического доступа к важнейшим ресурсам"), а не то, каким образом им следует обеспечивать безопасность (например, "использовать двухфакторную аутентификацию"), что в свою очередь позволит правительству и отрасли пользоваться преимуществами постоянных улучшений в сфере безопасности. Кроме того,

ориентированный на результаты подход к разработке этих базовых уровней оставляет возможности и для их применения в конкретных секторах, а также для руководящих указаний в отношении способов, благодаря чему предприятия получат большую свободу в вопросах регулярного обновления собственных руководящих указаний, с тем чтобы они отражали изменяющуюся ситуацию в области технологий и угроз.

5.4.4 Использование широкого спектра рыночных рычагов

В стратегии должен рассматриваться широкий круг мер политики, позволяющих эффективно стимулировать все организации и отдельных лиц к выполнению их конкретных обязанностей в области кибербезопасности при соизмерении их с существующими рисками в соответствии с принципом всеобъемлющего подхода и ориентированных на конкретные особенности приоритетов (раздел 4.2).

Выявление несоответствий между тем, что рынки могут и должны поощрять, и тем, чего требует ситуация с точки зрения безопасности, является важнейшим шагом на пути к определению того, когда и как следует применять имеющийся спектр мер стимулирования и сдерживания в целях укрепления безопасности. В целях поощрения внедрения стандартов и практических методов в области кибербезопасности для CI и CII в стратегии следует указать, что правительство рассмотрит ряд возможных политических мер и рыночных рычагов, имеющихся в его распоряжении.

5.4.5 Налаживание государственно-частного партнерства

Стратегия должна поощрять налаживание официальных государственно-частных партнерских отношений в целях укрепления безопасности CI и CII. Государственно-частное партнерство является краеугольным камнем эффективной защиты важнейшей инфраструктуры и управления рисками в области безопасности как в краткосрочной, так и в долгосрочной перспективе. Оно играет незаменимую роль в укреплении доверительных отношений между представителями отрасли и правительством.

Тем не менее создание устойчивых партнерских форматов требует четкого понимания всеми заинтересованными участниками целей партнерства и взаимных преимуществ в области безопасности, создаваемых в процессе совместной работы. Некоторые из направлений могут включать: достижение согласия в отношении общих базовых уровней кибербезопасности, учреждение эффективных координационных структур, процессов и протоколов обмена информацией, укрепление доверия, формулирование идей, подходов и передовой практики в целях укрепления безопасности и обмен ими, а также улучшение координации на международном уровне.

Дополнительные справочные материалы перечислены на стр. 63 и 64.

5.5 Тематическая область 5 – Развитие возможностей, создание потенциала и повышение осведомленности

При обсуждении проблем кибербезопасности основное внимание уделяется вопросам технологий и политики, при этом упускается из виду человеческий фактор, который имеет основополагающее значение. Данная тематическая область охватывает задачи, связанные с поощрением создания потенциала и повышения осведомленности в области кибербезопасности среди государственных структур, граждан, частных предприятий и других организаций, которые играют важнейшую роль в создании условий для цифровой экономики в стране.

В качестве примеров передового опыта в настоящем разделе рассматривается разработка специальных учебных программ и программ повышения осведомленности в области кибербезопасности, расширение планов подготовки и программ по повышению квалификации работников, применение международных схем сертификации и содействие инновациям и созданию кластеров для научных исследований и разработок.

5.5.1 Разработка учебных программ в области кибербезопасности

Стратегия должна способствовать разработке школьных программ, направленных на ускоренное развитие навыков и повышение осведомленности в области кибербезопасности в системе формального образования. В частности, необходимо разрабатывать специальные учебные программы в области кибербезопасности для начальной и средней школы, включать курсы по кибербезопасности во все программы в области информатики и информационных технологий в высших учебных заведениях, вводить направления подготовки специалистов непосредственно в области кибербезопасности и организовывать соответствующие правительственные стажировки.

Кроме того, школьные учебные программы должны быть составлены таким образом, чтобы обеспечить осведомленность о профессиях в области кибербезопасности и стимулировать интерес к ним. В рамках дальнейших усилий в этом направлении правительству также следует рассмотреть возможность разработки различных систем поощрения, таких как стипендии на обучение по частным образовательным программам и гранты на соответствующие программы стажировок.

5.5.2 Стимулирование развития навыков и подготовки кадров

Стратегия должна предусматривать разработку программ обучения и повышения квалификации в области кибербезопасности для специалистов и неспециалистов из государственного и частного секторов. Эта деятельность может включать подготовку руководящих и оперативных кадров, организацию официальных стажировок и учебной практики, а также (государственную и международную) сертификацию специалистов в области безопасности, исходя из потребностей, определенных отраслевыми и правительственными организациями. Техническая подготовка должна дополняться инициативами в сфере управления рисками.

Стратегия также должна предусматривать разработку инициатив по развитию карьерных возможностей непосредственно в области кибербезопасности, в частности в государственном секторе, а также систем поощрения для увеличения числа квалифицированных специалистов по вопросам кибербезопасности. Такие инициативы и системы поощрения должны разрабатываться в партнерстве с представителями академических организаций, частного сектора и гражданского общества. В рамках усилий по повышению квалификации и подготовке кадров следует рассмотреть возможность применения подхода, основанного на принципе обеспечения гендерного баланса и призванного стимулировать, поощрять и упрощать привлечение большего числа женщин в целях преодоления существующего гендерного разрыва среди специалистов в области кибербезопасности и обеспечения открытости для всех в будущем.

5.5.3 Реализация согласованной программы по повышению осведомленности в области кибербезопасности

В стратегии должен быть определен компетентный орган, на который возлагается ответственность за координацию кампаний и мероприятий по повышению осведомленности в области кибербезопасности на национальном уровне, с тем чтобы обеспечить рациональное распределение ресурсов и установить подотчетность. Этот орган должен сотрудничать с соответствующими заинтересованными сторонами в разработке и

реализации программ по повышению осведомленности в области кибербезопасности, направленных на распространение информации о рисках и угрозах в этой сфере, а также о передовом опыте противодействия им.

Программа по повышению осведомленности в области кибербезопасности может включать кампании по привлечению внимания общественности, ориентированные на широкие слои населения, детей и лиц, испытывающих трудности в использовании цифровых технологий, а также нацеленные на потребителя образовательные программы и, в частности, инициативы по повышению осведомленности среди сотрудников руководящего звена в государственном и частном секторах.

5.5.4 Содействие инновациям, научным исследованиям и разработкам в области кибербезопасности

В стратегии должно предусматриваться формирование среды, способствующей проведению фундаментальных и прикладных исследований в области кибербезопасности в различных секторах и разными группами заинтересованных сторон. Например, могут быть реализованы следующие инициативы: проведение исследований на национальном уровне в поддержку целей, предусмотренных в национальной стратегии в области кибербезопасности; создание программ научных исследований и разработок в области кибербезопасности в государственных исследовательских организациях; эффективное распространение новых знаний, базовых технологий, методов, процессов и инструментов. Более того, в рамках осуществления стратегии государства также должны налаживать связи с международным исследовательским сообществом в научных областях, связанных с кибербезопасностью, таких как информатика, электротехника, прикладная математика и криптография, а также в гуманитарных областях, таких как социология, политология, бизнес и управление, психология и многие другие.

В стратегии должны рассматриваться возможные механизмы поощрения, такие как гранты, материально-техническое обеспечение, налоговые вычеты, конкурсы и другие инициативы, направленные на поощрение разработки инновационных решений, продуктов и услуг в области кибербезопасности.

Дополнительные справочные материалы перечислены на стр. 64 и 65.

5.6 Тематическая область 6 – Законодательство и регулирование

Эта тематическая область охватывает вопросы разработки нормативно-правовой базы для защиты общества от киберпреступности и содействия формированию безопасной и надежной киберсреды в соответствии с принципами открытости для всех и обеспечения доверительной среды (разделы 4.3 и 4.9 соответственно). Разработка нормативно-правовой базы может подразумевать принятие законов, в которых устанавливается значение понятия незаконной кибердеятельности; юридическое признание прав личности и гражданских свобод; создание механизмов соблюдения; создание потенциала для обеспечения соблюдения законов; институционализацию важнейших структур и международное сотрудничество по борьбе с киберпреступностью.

5.6.1 Разработка законодательства по борьбе с киберпреступностью

В стратегии должны предусматриваться меры по содействию разработке внутренней правовой базы, в которой будет дано четкое определение запрещенной кибердеятельности, в целях снижения уровня онлайновой преступности. Создание потенциала в этой сфере, как правило, подразумевает разработку правовой базы в области борьбы с киберпреступностью; для этого требуется принятие новых соответствующих законов и изменение существующих (например, уголовного кодекса, законов, регулирующих банковскую деятельность, электросвязь и другие сферы деятельности).

Стратегия также должна предусматривать разработку процесса, который позволит вести мониторинг соблюдения и пересмотра законодательства, а также работы механизмов управления, выявлять пробелы и дублирование функций различных органов, определять сферы, требующие модернизации, и устанавливать их приоритетность (например, существующее законодательство, в частности устаревшие законы в области электросвязи).

5.6.2 Признание и защита прав и свобод личности

В стратегии должны быть предусмотрены основные надлежащие процедурные гарантии (в случае уголовного расследования и преследования), а также права на защиту данных, включая обеспечение конфиденциальности личных данных (например, с помощью разработки нормативно-правовой базы в области защиты данных и конфиденциальности) и свобода выражения мнений в соответствии с принципом соблюдения основополагающих прав человека (раздел 4.5).

5.6.3 Создание механизмов соблюдения

В стратегии должны быть предусмотрены меры по созданию внутренних механизмов соблюдения (меры по обеспечению исполнения, а также меры поощрения). Внедрение этих механизмов необходимо для предотвращения и пресечения действий, предпринимаемых с целью подрыва конфиденциальности, целостности и доступности систем и инфраструктуры ИКТ и угрожающих компьютерным данным, а также для смягчения последствий этих действий в соответствии с вышеупомянутой нормативно-правовой базой. В этих механизмах среди прочего должны учитываться особенности цифрового расследования, законного перехвата сообщений и использования электронных доказательств.

5.6.4 Содействие созданию потенциала в области правоприменительной деятельности

Стратегия должна способствовать развитию потенциала, связанного с правоприменительной деятельностью в области кибербезопасности, включая подготовку и обучение для различных заинтересованных сторон, участвующих в борьбе с киберпреступностью (например, для судей, прокуроров, адвокатов, сотрудников правоохранительных органов, криминалистов и других специалистов, участвующих в расследованиях). Сотрудники правоохранительных органов должны пройти специальную подготовку, чтобы уметь толковать и применять внутренние законы в области противодействия киберпреступности (т. е. толковать законы с точки зрения технических понятий и наоборот), эффективно выявлять, предотвращать, расследовать киберпреступления и привлекать к ответственности лиц, виновных в этих преступлениях, а также осуществлять эффективное сотрудничество с отраслевыми и международными правоохранительными структурами (такими как ИНТЕРПОЛ и Европол) в целях противодействия киберпреступности и укрепления кибербезопасности. Деятельность в этом направлении должна осуществляться с учетом тематической области 5, касающейся расширения возможностей, создания потенциала и повышения осведомленности (раздел 5.5).

5.6.5 Налаживание взаимодействия между организациями

В стратегии должен быть определен и признан мандат национальных учреждений, которые несут главную ответственность за обеспечение соблюдения законодательства в области противодействия киберпреступности, защиту важнейших объектов инфраструктуры и контроль за выполнением всех международных требований в области борьбы с киберпреступностью (например, обеспечение соответствия национальных законов международным договорным обязательствам), в том числе по линии судебных ведомств (например, трансграничное сотрудничество) (см. также разделы 5.1.3, 5.1.4 и 5.6.6).

В рамках некоторых правовых систем для учреждения органов по обеспечению кибербезопасности, таких как национальные CERT/CIRT/CSIRT, или для наделения какого-то одного ведомства полномочиями по координации политики в области кибербезопасности в стране может потребоваться принятие соответствующих законов.

5.6.6 Поддержка международного сотрудничества по борьбе с киберпреступностью

В стратегии должна быть отражена приверженность государства защите общества от киберпреступности на глобальном уровне путем ратификации (если это представляется возможным и соответствует общей национальной повестке дня) международных соглашений по противодействию киберпреступности или аналогичных соглашений по борьбе с киберпреступностью, а также путем оказания содействия механизмам координации в области борьбы с международной киберпреступностью. В частности, может потребоваться приведение национальных законов в соответствие с международными договорными обязательствами и двусторонними соглашениями, например, путем создания системы правовой взаимопомощи, условий для осуществления трансграничных расследований и уголовного преследования, обработки цифровых доказательств и экстрадиции.

Деятельность в этом направлении должна осуществляться с учетом тематической области 7, касающейся международного сотрудничества (раздел 5.7).

Дополнительные справочные материалы перечислены на стр. 65 и 66.

5.7 Тематическая область 7 – Международное сотрудничество

В этой тематической области рассматриваются аспекты, касающиеся внешних обязательств конкретной страны в области кибербезопасности на региональном и международном уровнях, которые должны охватываться стратегией. Кибербезопасность играет все более важную роль во множестве различных областей международных отношений, включая права человека, экономическое развитие, торговлю, коммерческую деятельность, контроль над вооружениями, безопасность, стабильность, поддержание мира и разрешение конфликтов.

Таким образом, в стратегии должно признаваться, что в вопросах обеспечения кибербезопасности не существует границ, поэтому необходимо сотрудничать с заинтересованными сторонами не только на национальном, но и на международном уровне. Международное сотрудничество с заинтересованными сторонами из государственного и частного секторов имеет ключевое значение в содействии конструктивному диалогу, развитии механизмов укрепления доверия и сотрудничества, поиске взаимоприемлемых решений для общих проблем и создании глобальной культуры кибербезопасности.

В соответствии с принципом всеобъемлющего подхода и приоритетами, ориентированными на конкретные особенности стран (раздел 4.2), региональное и международное сотрудничество должно развиваться с учетом особенностей политического, общественного, культурного и экономического устройства страны, а также приоритетных направлений ее внешней политики.

5.7.1 Признание важного значения кибербезопасности как одного из приоритетов внешней политики

В стратегии следует подчеркнуть приверженность государства международному сотрудничеству в области кибербезопасности и признать вопросы обеспечения кибербезопасности неотъемлемым компонентом внешней политики страны. В связи с этим важно поощрять развитие и применение компетенций и навыков в области обеспечения кибербезопасности (кибердипломатии) в дополнение к традиционным дипломатическим методам и процессам. Стратегия также может подразумевать развитие отдельных организационных структур, а также создание специального управления или назначение квалифицированных сотрудников, которые будут отвечать за дипломатическое взаимодействие по вопросам кибербезопасности.

В частности, в стратегии следует четко установить направления работы правительства и долгосрочные задачи в области международного сотрудничества, а также указать, с какими заинтересованными сторонами (представителями государственного или частного сектора, на региональном или глобальном уровне) будет осуществляться взаимодействие. Эти направления и задачи могут включать среди прочего оказание поддержки в разработке международных норм и мер по укреплению доверия в области кибербезопасности, приверженность созданию потенциала в области обеспечения кибербезопасности, участие в разработке международных стандартов в области кибербезопасности, а также присоединение к действующим региональным и международным нормативно-правовым актам.

Может также потребоваться более эффективное согласование деятельности между различными правительственными субъектами (такими как глава государства или правительства, министерство иностранных дел, министерство ИКТ, министерство промышленности и торговли, министерство юстиции, министерство обороны и т. д.), с тем чтобы политическая позиция, которая озвучивается одной из внутренних заинтересованных сторон в ходе международных переговоров по вопросам кибербезопасности, была должным образом согласована с другими государственными органами.

5.7.2 Участие в международных обсуждениях

В стратегии должны быть определены конкретные международные форумы и механизмы сотрудничества, к которым государство намерено присоединиться в целях эффективного дипломатического взаимодействия по вопросам кибербезопасности, включая региональные или международные организации, межправительственные дискуссии, объединения государственного и/или частного сектора, а также традиционные отлаженные механизмы сотрудничества и взаимодействия, в рамках которых, в частности, затрагиваются вопросы кибербезопасности.

По мере осуществления сотрудничества правительству, вероятнее всего, потребуется принять меры по развитию дополнительных компетенций и навыков, направленные на укрепление общего потенциала страны в области кибербезопасности. В связи с этим важно эффективным образом определить приоритетный порядок этих усилий и выделить необходимые ресурсы (людские и финансовые) в целях получения конкретных результатов.

5.7.3 Поощрение официального и неофициального сотрудничества в киберпространстве

В стратегии должны быть указаны оперативные механизмы международного сотрудничества, к которым намерено присоединиться государство. Государство может принимать участие в официальных или неофициальных международных инициативах, направленных на развитие сотрудничества в таких областях, как разработка политики и законодательства, охрана правопорядка, реагирование на инциденты, обмен информацией, в том числе информацией об угрозах. Участие в подобных инициативах, в частности, может способствовать повышению эффективности сотрудничества и обмена информацией о потенциальных угрозах и факторах уязвимости между соответствующими органами.

5.7.4 Согласование национальных и международных усилий по обеспечению кибербезопасности

В стратегии должны учитываться существующие региональные и международные инициативы в области кибербезопасности и предусматриваться меры по содействию гармонизации и согласованию. Это позволит государству использовать существующие передовые методы работы и вносить вклад в достижение единообразия и сближение подходов к обеспечению кибербезопасности.

В связи с этим в стратегии должна быть отражена приверженность государства обеспечению согласованности между внутренним законодательством и внешнеполитической повесткой дня; для этого ему следует привести национальную нормативно-правовую базу и политику в соответствие с его международными обязательствами, а также обеспечить согласованность национальных подходов к обеспечению кибербезопасности с его усилиями на международном уровне.

В стратегии могут быть рассмотрены наиболее значимые примеры усилий, осуществляемых на международном уровне, включая следующие (но не ограничиваясь ими): работа Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН); деятельность Организации по безопасности и сотрудничеству в Европе (ОБСЕ) в области мер по укреплению доверия и международных норм, применимых к киберпространству; работа Подгруппы по преступлениям с использованием высоких технологий Группы семи; Конвенция Совета Европы о киберпреступности, принятая в Будапеште; Конвенция Африканского союза о кибербезопасности; Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности; Конвенция о борьбе с преступлениями в области информационных технологий Лиги арабских государств; Директива ЭКОВАС по борьбе с киберпреступностью; поддержка Таллиннского руководства 1.0 и 2.0 Экспертным центром НАТО по совместной кибероборонe (CCD COE).

Дополнительные справочные материалы перечислены на стр. 66.

6 Справочные материалы

В ходе разработки настоящего руководства был проведен анализ существующих руководящих указаний и передового опыта.

Это позволило нам определить уже имеющиеся материалы, которые могут послужить подспорьем в разработке государствами национальных стратегий кибербезопасности. Ниже приводится исчерпывающий перечень этих материалов, включая веб-ссылки.

CCI (2017), Harare Scheme on Mutual Legal Assistance in Criminal Matters

Carnegie Mellon (2003), Handbook for Computer Security Incident Response Teams (CSIRTs)

Commonwealth (2018), Commonwealth Cyber Declaration

CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies

Совет Европы (2001 г.), Конвенция Совета Европы о киберпреступности (Будапештская конвенция)

Council of the European Union (2017), Cyber Diplomacy toolbox

ENISA (2014), An Evaluation Framework For National Cyber Security Strategies

ENISA (2011), CERT Operational Gaps and Overlaps

ENISA (2011), Good Practice Guide for Incident Management

ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services

ENISA (2016), National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies

ENISA (2012), National Cyber Security Strategies: Practical Guide on Development and Execution

ENISA (2012), National Cyber Security Strategy, Setting the Course for National Efforts to Strengthen Security in Cyberspace

ENISA (2016), National Cyber Security Strategies: Training Tool

ENISA (2016), Stocktaking, Analysis and Recommendations on the Protection of CIIs

ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation

Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations

МСЭ (2017 г.), Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

МСЭ (2017), Глобальный индекс кибербезопасности

МСЭ (2011), Руководство по национальным стратегиям кибербезопасности

МСЭ (2010 г.), ПОНИМАНИЕ КИБЕРПРЕСТУПНОСТИ: явление, задачи и законодательный ответ

МСЭ (2009 г.), Руководство по кибербезопасности для развивающихся стран

Microsoft (2013), Developing a National Strategy for Cybersecurity

Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum

Microsoft (2014), Critical Connections: Protecting Infrastructures

Microsoft (2014), Hierarchy of Cybersecurity Needs

Microsoft (2018), Building an effective national cybersecurity agency

Microsoft (2018), Cybersecurity Policy Framework

Microsoft (2015), Information Sharing Framework for Cybersecurity

Microsoft (2017), Risk Management for Cybersecurity: Security Baselines

NATO CCD COE (2012), National Cyber Security Framework Manual

NATO CCD COE (2013), National Cyber Security Strategy Guidelines

NIST (2014), Framework for Improving Critical Infrastructure Cybersecurity

OAS (2015), Best Practice for Establishing a National CSIRT

OAS (2004), Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity

OAS (2015), Cyber Security Awareness Campaign Toolkit

OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas

OECD (2015), Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity

OECD (2012), Cybersecurity Policy Making at a Turning Point

OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity

ОЭСР (2013 г.), Рекомендации Совета, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных

OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures

OECD (2007), Report on the Development of Policies for the Protection of Critical

Information Infrastructures

Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0. План киберготовности: доклад и индекс

Организация Объединенных Наций (2015 г.), Цели в области устойчивого развития

Организация Объединенных Наций (1976 г.), Международный пакт об экономических, социальных и культурных правах, Международный пакт о гражданских и политических правах и Факультативный протокол к Международному пакту о гражданских и политических правах, резолюция
2200 (XXI)

Организация Объединенных Наций (2014 г.), Право на неприкосновенность личной жизни в цифровой век, резолюция A/RES/68/167

Организация Объединенных Наций (1948 г.), Всеобщая декларация прав человека

UNCTAD (2014), A Framework for Information and Communications Technology Policy Reviews

UNCTAD, Developing E-Commerce Legislation

UNCTAD (2016), Study on Data Protection Regulations and International Data Flows

КПЧ ООН (1976 г.), Международный пакт о гражданских и политических правах

World Bank et al (2017), Combatting Cybercrime: Tools and Capacity Building for Emerging Economies

Ниже представлена подробная разбивка материалов по отдельным принципам и областям передового опыта.

Жизненный цикл национальной стратегии в области кибербезопасности

Подтема	Справочные материалы
Инициирование	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3
Обзор и критический анализ имеющегося опыта	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 2.1, 2.2, 3.2.1, 3.3.1 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 4
Разработка национальной стратегии	ENISA (2016), National Cyber Security Strategies: Training Tool
Осуществление	ENISA (2016), National Cyber Security Strategies: Training Tool
Мониторинг и оценка	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.9 NATO CCD COE (2012): National Cyber Security Framework Manual, section: 2.4

Всеобъемлющие принципы

Подтема	Справочные материалы
Концепция	Microsoft (2013), Developing a National Cybersecurity Strategy, p.4
	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1
	OECD (2015), Recommendation on Digital Security Risk Management for Economic and Social Prosperity
	Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0. План киберготовности: доклад и индекс, стр. 1–3 английского оригинала
Всеобъемлющий подход и ориентированные на конкретные особенности приоритеты	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
Открытость для всех	CCI (2013), Checklist p2
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies 4.5 and 4.6.6
	ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services, chapter 3
	ENISA (2016), An Evaluation Framework for National Cyber Security Strategies 3.2
	ENISA (2016), National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace, p.9
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14
	МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, раздел 5.3
	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.1.3
	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 3.5, 4.3
	OAS (2015), Cyber Security Awareness Campaign Toolkit, p.20

Подтема	Справочные материалы
Открытость для всех *(продолж.)*	OAS (2015), Report on Cybersecurity and Critical Infrastructure in the Americas, p.2 OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p.14-15 ОЭСР (2013 г.), Рекомендации Совета, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных; Дополнительная пояснительная записка к пересмотренному Руководству ОЭСР по защите неприкосновенности частной жизни, стр. 31 английского оригинала Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0. План киберготовности: доклад и индекс, стр. 2–6 английского оригинала UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development UNCTAD (2014), A Framework for Information and Communications Technology Policy Reviews
Экономическое и социальное процветание	Microsoft (2014), Hierarchy of Cybersecurity Needs, chapter 1 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.1, 2.2.1 Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0. План киберготовности: доклад и индекс, стр. 1–3 английского оригинала
Основополагающие права человека	CCI (2013), Checklist 2.6.5. CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, Principle 4 ENISA (2014), An Evaluation Framework for Cyber Security Strategies, 3.1.1 Objectives Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, p.39 МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, раздел 7.4 Microsoft (2013), Developing a National Cybersecurity Strategy, p.5

Подтема	Справочные материалы
Основополагающие права человека *(продолж.)*	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 1.3.1, 1.3.3
	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.4, 1.5.5, 5.2.6
	OECD (2015), Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity, principle 9 and principle 3
	UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development
	Организация Объединенных Наций (1948 г.), Всеобщая декларация прав человека
	Организация Объединенных Наций (1976 г.), Международный пакт об экономических, социальных и культурных правах, Международный пакт о гражданских и политических правах и Факультативный протокол к Международному пакту о гражданских и политических правах
	Организация Объединенных Наций (2014 г.), Право на неприкосновенность личной жизни в цифровой век
Управление рисками и устойчивость	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	Global Cyber Security Capacity Centre, University of Oxford(2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.15
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.6
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	OECD (2015), Recommendation on Digital Security Risk Management Economic and Social Prosperity and Companion Document
Надлежащий набор политических инструментов	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.1
	NATO CCD COE (2012): National Cyber Security Framework Manual, section: 1.4

Подтема	Справочные материалы
Четкое руководство, функции и распределение ресурсов	ENISA (2016), NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies NATO CCD COE (2012): National Cyber Security Framework Manual, section: 4 Microsoft (2018): Building an effective national cybersecurity agency Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0. План киберготовности: доклад и индекс, разделы 1–7
Доверительная среда	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 2.2, p.25 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, разделы 4, 6

Передовая практика, касающаяся национальной стратегии в области кибербезопасности

Подтема	Справочные материалы
Тематическая область 1 – Управление	CCI (2013), Checklist. CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.1, 4.4.4, 4.4.5, 4.4.8, 4.4.9, 4.4.20, 4.4.21, 4.4.34, 4.5 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.1, 3.2, 3.4, 3.5, 3.17 ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, sections: 2.2.1, 3.1.1, 3.1.2, 3.1.3 ENISA (2016), National Cyber Security Strategies: Setting the course for National Efforts to Strengthen Security in Cyberspace, sections: 4, 6 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, 1.5, 1.6, p.14-15 МСЭ (2011 г.): Руководство по национальным стратегиям кибербезопасности, разделы 5.2.1, 5.3, 7.2, 7.3, 11.1, 11.2, 20, 20.2 Microsoft (2013), Developing a National Cybersecurity Strategy, sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline Microsoft (2018) Building an effective national cybersecurity agency NATO CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.1, 3.3, 3.8 NATO CCD COE (2012), National Cyber Security Framework Manual, sections: 1.4.2, 2.1.1 2.1.3, 2.2, 2.3, 2.4, 3.1, 3.5, 4, 5.3.1 OECD (2012), Cybersecurity Policy Making at a Turning Point, Annex IV ОЭСР (2013 г.), Рекомендации Совета, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document

Подтема	Справочные материалы
Тематическая область 1 – Управление *(продолж.)*	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, раздел 1
Тематическая область 2 – Управление рисками в области национальной кибербезопасности	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.6, 4.4.15, 4.4.24, 4.4.25, 4.4.26, 4.4.27 ENISA (2016), National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.3 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.14 МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, раздел 10.1.2 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2013), Developing a National Cybersecurity Strategy, chapter on Building a Risk Approach NATO CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.5 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 2.1.2, 5.3.2 NIST (2015), Framework for Improving Critical Infrastructure Cybersecurity OAS (2018), Managing National Cyber Risk OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, раздел 1

Подтема	Справочные материалы
Тематическая область 3 – Обеспечение готовности и устойчивости	Carnegie Mellon (2003), Handbook for Computer Security Incident Response Teams (CSIRTs)
	CCI (2013), Checklist
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, section: 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31
	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.6, 3.7, 3.10, 3.14, 4.1, 4.5, 4.8
	ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, p.
	ENISA (2011), CERT Operational Gaps and Overlaps, p.
	ENISA (2011), Good Practice Guide for Incident Management, p.
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.2, p.14
	МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности: 11.3, 17.3
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	Microsoft (2015), Information Sharing Framework for Cybersecurity
	Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Building Incident Response Capabilities
	NATO CCD COE (2013): National Cyber Security Strategy Guidelines, Section: 3.5
	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.2, 4.2.2
	OAS (2016), Best Practice for Establishing a National CSIRT, p.35
	OAS (2004), Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, pp.3-4
	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B
	Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, разделы 2, 4

Подтема	Справочные материалы
Тематическая область 4 – Услуги важнейшей инфраструктуры/ необходимые услуги	СТО (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.12, 4.4.13, 4.4.20, 4.4.25, 4.4.26, 4.4.28, 4.4.32 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, 1.4, p.14; Dimension 5.2, p.49 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, section: 4.2 МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, разделы 5.1.1, 5.3.3, 11.4 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum, all sections Microsoft (2014), Critical Connections: Protecting Infrastructures, all sections NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 3.4, 3.5 NATO CCD COE (2012), National Cyber Security Framework Manual, section: 4.5.4 OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures: Part I, Part II Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, разделы 2, 4

Подтема	Справочные материалы
Тематическая область 5 – Развитие возможностей, создание потенциала и повышение осведомленности	CCI (2013), Checklist; CCI (2005, 2017), Commonwealth Network of Contact Persons Framework; CCI (2011), Harare Scheme on Mutual Legal Assistance in Criminal Matters; CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.11, 4.4.17, 4.4.20, 4.4.34, 4.4.12, 4.4.14, 4.4.16, 4.4.23 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.12, 3.8, 3.11, 3.13, 4.3, 4.6, 4.7, 4.14 ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, section: 2.1 ENISA (2011), CERT Operational Gaps and Overlaps, p.6, 16, 19, 21, 27, 29, 31, 32, 50, 57 ENISA (2010), Good Practice Guide for Incident Management, p.19, 23, 26, 32, 46, 56, 58, 64, 69 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.5, p.15; Dimension 2.1, 2.2, 2.3, p.25; Dimension 3-1, 3-2, 3-3, p. 32; Dimension 5.6, p.49 МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, разделы 5.3.7, 5.3.8, 12.4, 12.1, 12.3, 18 Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Driving Research and Technology Investment, Public Awareness, Workforce Training and Education; NATO CCD COE (2013, National Cyber Security Strategy Guidelines, section: 3.5 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.5.5, 4.6.3; OAS (2015), Cyber Security Awareness Campaign Toolkit, all sections; OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B

Подтема	Справочные материалы
Тематическая область 5 – Развитие возможностей, создание потенциала и повышение осведомленности *(продолж.)*	Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, разделы 2, 5 UNCTAD (2015), Prgramme on E-Commerce and Law Reform
Тематическая область 6 – Законодательство и регулирование	CCI (2013), Checklist CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20 Совет Европы (2001 г.), Конвенция Совета Европы о киберпреступности (Будапештская конвенция), статья 15 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.15, 3.184.9, 4.12 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, 4.2, 4.3, p.39-40; Dimension 5.7, p.50 КПЧ ООН (1976 г.), Международный пакт о гражданских и политических правах, статья 19 МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, разделы 5.3.4, 5.3.5, 9, 11.5, 12.2, 15 МСЭ (2010 г.), Комплект материалов МСЭ по законодательству в области киберпреступности NATO CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.2 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, section: 5 OAS: Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, раздел 3 Организация Объединенных Наций (2015 г.), Цели в области устойчивого развития, статья 16.3

Подтема	Справочные материалы
Тематическая область 6 – Законодательство и регулирование *(продолж.)*	UNCTAD, Global Cyberlaw Tracker World Bank et al., Combatting Cybercrime: Tools andCapacity Building for Emerging Economies
Тематическая область 7 – Международное сотрудничество	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.20, 4.4.21 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.16 and 4.10 ENISA (2016), Guidebook on National Cyber Security Strategies, section: 3.16 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.3, p.40 МСЭ (2011 г.), Руководство по национальным стратегиям кибербезопасности, разделы 5.3.9, 10.2.2, 13, 19 Microsoft (2013), Developing a National Strategy for Cybersecurity, section on structuring international engagement NATO CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.3, 3.2.1, 3.3.2 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.7, 5.4.2, 5.4.3 OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, chapters: 4, 5 OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p. 13, 48, 58 Потомакский институт политических исследований (2015 г.), Индекс киберготовности 2.0, разделы 4, 6

7 Список сокращений

Сокращение	Значение
CCI	Инициатива Содружества по борьбе с киберпреступностью
CERT	Группа реагирования на нарушения компьютерной защиты
CBM	Меры по укреплению доверия
CII	Важнейшая информационная инфраструктура
ОЭС	Организация по электросвязи Содружества
ENISA	Европейское агентство по сетевой и информационной безопасности
ИКТ	Информационно-коммуникационные технологии
МСЭ	Международный союз электросвязи
NATO CCD COE	Экспертный центр НАТО по совместной кибероборонe
NIST	Национальный институт стандартов и технологий
ОАГ	Организация американских государств
ОЭСР	Организация экономического сотрудничества и развития
ООН	Организация Объединенных Наций
ЮНКТАД	Конференция ООН по торговле и развитию

ISBN: 978-92-61-27794-9