Стратегическое взаимодействие в области кибербезопасности

Руководство по разработке национальной стратегии кибербезопасности

Издание второе, 2021 год

Партнеры


COUNCIL OF EUROPE
CONSEIL DE L'EUROPE


The Commonwealth


CTO
COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION


DCAF
Geneva Centre
for Security Sector
Governance


Deloitte.


FIRST


Global
Cyber Security
Capacity Centre


GCSP
Geneva Centre for
Security Policy


GLOBAL
PARTNERS
DIGITAL


INTERPOL


ITU


Microsoft


CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE


THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Наблюдатели

Некоторые права защищены

Настоящее Руководство разработано при участии двадцати партнеров из числа межправительственных и международных организаций, предприятий частного сектора, а также научных учреждений и организаций гражданского общества. В это число вошли: Совет Европы (СЕ), Секретариат Британского Содружества (ComSec), Организация по электросвязи Британского Содружества (СТО), Женевский центр управления сектором безопасности (DCAF), Международная сеть компаний Deloitte, Форум групп реагирования на инциденты и обеспечения безопасности (FIRST), Глобальный центр развития потенциала в области кибербезопасности (GCSCC), Женевский центр политики в области безопасности (GCSP), компания Global Partners Digital (GPD), Международная организация уголовной полиции (Интерпол), Международный союз электросвязи (МСЭ), компания Microsoft, Центр передового опыта по совместной защите от киберугроз при НАТО (CCDCOE), Потомакский институт политических исследований (PIPS), Исследовательский центр RAND Europe, Всемирный банк, Институт Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), Контртеррористическое управление Организации Объединенных Наций (КТУ ООН), Университет Организации Объединенных Наций (УООН). Вклад в разработку Руководства в качестве наблюдателей внесли организация Axon Partners Group (Axon), Институт киберготовности (CRI), Глобальный форум по киберкомпетентности (GFCE), Организация американских государств (ОАГ) и Всемирный экономический форум (ВЭФ). Далее все вышеупомянутые организации совместно именуются "Авторы".

Права и разрешения

Перевод – при выполнении перевода настоящей работы просьба добавить следующую правовую оговорку наряду с указанием авторства: *Совет Европы (СЕ), Секретариат Британского Содружества (ComSec), Организация по электросвязи Британского Содружества (СТО), Женевский центр управления сектором безопасности (DCAF), Международная сеть компаний Deloitte, Форум групп реагирования на инциденты и обеспечения безопасности (FIRST), Глобальный центр развития потенциала в области кибербезопасности (GCSCC), Женевский центр политики в области безопасности (GCSP), компания Global Partners Digital (GPD), Международная организация уголовной полиции (Интерпол), Международный союз электросвязи (МСЭ), компания Microsoft, Центр передового опыта по совместной защите от киберугроз при НАТО (CCDCOE) , Потомакский институт политических исследований (PIPS), Исследовательский центр RAND Europe, Всемирный банк, Институт Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), Контртеррористическое управление Организации Объединенных Наций (КТУ ООН), Университет Организации Объединенных Наций (УООН) не участвовали в создании настоящего перевода. Вышеупомянутые организации не несут ответственности за содержание этого перевода и за ошибки, допущенные при переводе.*

Адаптация – при адаптации настоящей работы просьба добавить следующую правовую оговорку наряду с указанием авторства. Данный текст является адаптацией оригинальной работы, авторами которой являются Совет Европы (СЕ), Секретариат Британского Содружества (ComSec), Организация по электросвязи Британского Содружества (СТО), Женевский центр управления сектором безопасности (DCAF), Международная сеть компаний Deloitte, Форум групп реагирования на инциденты и обеспечения безопасности (FIRST), Глобальный центр развития потенциала в области кибербезопасности (GCSCC), Женевский центр политики в области безопасности (GCSP), компания Global Partners Digital (GPD), Международная организация уголовной полиции (Интерпол), Международный союз электросвязи (МСЭ), компания Microsoft, Центр передового опыта по совместной защите от киберугроз при НАТО (CCDCOE), Потомакский институт политических исследований (PIPS), Исследовательский центр RAND Europe, Всемирный банк, Институт Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), Контртеррористическое управление Организации Объединенных Наций (КТУ ООН), Университет Организации Объединенных Наций (УООН*). Мнения и точки зрения, выраженные при адаптации, являются исключительной ответственностью автора или авторов адаптации и не одобряются вышеуказанными организациями.*

Сторонний контент – авторы не обязательно владеют каждым компонентом контента, содержащегося в настоящей работе. Поэтому они не гарантируют, что использование в этой работе какого-либо отдельного компонента или части, принадлежащих третьим лицам, не будет нарушать права этих третьих лиц. Риск предъявления претензий, связанных с таким нарушением, лежит исключительно на вас. Если вы захотите повторно использовать какой-либо компонент работы, вы несете ответственность за определение того, требуется ли разрешение на такое повторное использование, и получить его от владельца авторских прав. Примерами компонентов являются, помимо прочего, таблицы, рисунки и фотографии.

Любые запросы на использование, выходящие за рамки вышеупомянутой лицензии (CC BY-NC 3.0 IGO), следует направлять в Международный союз электросвязи (МСЭ) по адресу: Place des Nations, 1211 Geneva 20, Switzerland; эл. почта: itumail@itu.int.

Правовые оговорки; привилегии и иммунитеты

Выводы, интерпретации и заключения, изложенные в настоящей публикации, не обязательно отражают точку зрения авторов, их секретариатов или руководящих органов. Авторы не гарантируют точность данных, включенных в эту работу. Границы, цвета, названия и другая информация, показанные на любом графике или диаграмме в этой работе, не подразумевают никакого суждения со стороны МПО относительно правового статуса какой-либо территории, одобрения или принятия таких границ.

Ничто в настоящем документе не должно представлять собой или рассматриваться как ограничение или отказ от привилегий и иммунитетов, на которые определенные авторы имеют право в соответствии с национальными законами и международными соглашениями; все они специально защищены.

Совместное предисловие

За последние два десятилетия люди во всем мире получали пользу от развития и внедрения информационно-коммуникационных технологий (ИКТ) и связанных с ними социально-экономических и политических возможностей. Цифровая трансформация может стать мощным фактором инклюзивного и устойчивого развития, но лишь в том случае, если базовая инфраструктура и зависящие от нее услуги безопасны, надежны и устойчивы. Чтобы воспользоваться преимуществами цифровизации и справиться с присущими ей проблемами, странам необходимо включить распространение инфраструктуры и услуг на основе ИКТ в рамки комплексной национальной стратегии кибербезопасности.

Чтобы помочь государственным учреждениям в этом начинании, консорциум партнерских организаций совместно подготовил и опубликовал в 2018 году первое Руководство по разработке национальной стратегии кибербезопасности (NCS). С тех пор количество национальных стратегий или структур кибербезопасности во всем мире значительно увеличилось. Если в 2018 году такую стратегию приняли только 76 стран, то сегодня подобные стратегии действуют более чем в 127 странах, и многие использовали Руководство в качестве справочного материала и плана действий[1].

Однако быстро меняющийся характер киберпространства, растущая зависимость от ИКТ и распространение цифровых рисков – все это требует постоянного совершенствования национальных стратегий кибербезопасности. Большинство стран ускорили процесс цифровой трансформации и все больше обеспокоены непосредственными и будущими угрозами своим критически важным службам, инфраструктурам, секторам экономики, учреждениям и предприятиям, а также миру и безопасности во всем мире, которые могут возникнуть в результате неправомерного использования цифровых технологий и недостаточной устойчивости. Это второе издание Руководства выходит в очень сложное время. Его обновленное содержание отражает усложненный и динамичный характер киберпространства, а также основные тенденции, которые могут повлиять на кибербезопасность и поэтому должны быть включены в национальное стратегическое планирование. Цель Руководства заключается в том, чтобы стимулировать стратегическое мышление и продолжать оказывать поддержку национальным руководителям и директивным органам в их текущей деятельности по разработке, созданию и реализации таких национальных стратегий и политики в области кибербезопасности. Мы уверены, что это новое Руководство послужит полезным инструментом для всех заинтересованных сторон, отвечающих за кибербезопасность.

Как и предыдущее издание, настоящее Руководство является результатом уникального совместного и равноправного многостороннего сотрудничества партнеров, работающих в области национальных стратегий, политики и наращивания потенциала в области кибербезопасности. Двадцать экспертных организаций из государственного и частного секторов, а также научных кругов и гражданского общества внесли свои опыт, знания и профессиональные компетенции в процесс подготовки этого обновленного Руководства, в котором использованы собственные ноу-хау участвующих организаций, а также приводятся ссылки на дополнительные публикации и другие доступные ресурсы.

Мы хотели бы выразить благодарность партнерам за их неоценимую поддержку и приверженность тому, чтобы этот проект стал примером успешного многостороннего сотрудничества. Мы хотим поощрять это партнерство к продолжению совместной работы и рассчитываем на еще более тесное сотрудничество с правительствами, региональными и международными органами, правоохранительными органами, академическими кругами, частным сектором, гражданским обществом и учреждениями Организации Объединенных Наций для содействия стратегическому анализу вопросов кибербезопасности, наращивания потенциала и устойчивости.

[1] Отчеты "Глобальный индекс кибербезопасности" за 2018 и 2020 годы. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Совместно подписано следующими лицами:

Г-н Хорхе Мартинес Морандо
Партнер, Axon Partners Group Consulting

Г-н Александр Зегер
Начальник отдела киберпреступности, Совет Европы

Г-жа Лесси Лонгстрит
Директор по международным связям и сотрудничеству с партнерами, Институт киберготовности

Д-р Луис Франчески
Старший директор Управления по вопросам управления и мира, Секретариат Британского Содружества

Г-жа Бернадетт Льюис
Генеральный секретарь Организации электросвязи Британского Содружества

Посол Томас Гербер
Директор Женевского центра управления сектором безопасности

Г-н Андреа Ригони
Партнер и руководитель направления кибербезопасности глобальных правительственных и государственных услуг, Deloitte

Г-н Крис Гибсон
Исполнительный директор, Форум групп реагирования на инциденты и обеспечения безопасности

Проф. Сэди Криз
Директор Глобального центра развития потенциала в области кибербезопасности

Посол Томас Гремингер
Директор Женевского центра политики безопасности

Г-н Дэвид ван Дурен
Директор Секретариата Международного форума по киберкомпетентности

Г-жа Леа Каспар
Исполнительный директор, Global Partners Digital

Г-н Крейг Джонс
Директор подразделения по киберпреступности, Интерпол

Г-жа Дорин Богдан-Мартин
Директор Бюро развития электросвязи, Международный союз электросвязи

Г-жа Аманда Крейг
Старший директор по политике кибербезопасности, Microsoft

Полковник Яак Тариен
Директор Центра передового опыта по совместной защите от киберугроз при НАТО

Г-жа Мелисса Хэтэуэй
Президент Hathaway Global Strategies LLC и старший научный сотрудник Потомакского института политических исследований

Г-жа Николь Клинген
Исполняющий обязанности директора по цифровому развитию, Всемирный банк

Д-р Робин Гейсс
Директор Института Организации Объединенных Наций по исследованию проблем разоружения

Д-р Джехангир Хан
Директор Контртеррористического центра Организации Объединенных Наций, Контртеррористическое управление Организации Объединенных Наций

Д-р Цзинбо Хуан
Директор института Университета Организации Объединенных Наций в Макао

Г-н Жорж де Моура
Руководитель направления отраслевых решений Центра кибербезопасности, Всемирный экономический форум

Содержание

Некоторые права защищены v
Права и разрешения v
Правовые оговорки; привилегии и иммунитеты vii
Совместное предисловие viii
Вступление 5
Примечание для читателей о внесенных изменениях 6
1 Обзор документа 7
1.1 Цель 8
1.2 Сфера применения 8
1.3 Общая структура и указания по использованию Руководства 9
1.4 Целевая аудитория 9
2 Введение 11
2.1 Что такое кибербезопасность 13
2.2 Преимущества национальной стратегии кибербезопасности и процесс ее разработки 13
3 Жизненный цикл национальной стратегии кибербезопасности 15
3.1 Этап I. Инициирование 16
3.1.1 Определение органа управления проектом 16
3.1.2 Учреждение руководящего комитета 18
3.1.3 Определение заинтересованных сторон для привлечения к разработке стратегии 19
3.1.4 Определение людских и финансовых ресурсов 19
3.1.5 Планирование разработки стратегии 20
3.2 Этап II. Критический обзор и анализ 20
3.2.1 Оценка общей ситуации в стране в области кибербезопасности 21
3.2.2 Оценка ситуации с киберрисками 22
3.3 Этап III. Разработка национальной стратегии кибербезопасности 22
3.3.1 Разработка проекта национальной стратегии кибербезопасности 22
3.3.2 Консультации с широким кругом заинтересованных сторон национального, регионального и международного уровней 23
3.3.3 Запрос официального одобрения 23
3.3.4 Публикация и продвижение стратегии 23
3.4 Этап IV. Реализация 24
3.4.1 Разработка плана действий 24
3.4.2 Определение инициатив, которые необходимо реализовать 24
3.4.3 Выделение людских и финансовых ресурсов для реализации стратегии 24
3.4.4 Установление сроков и показателей 25
3.5 Этап V. Контроль и оценка 25
3.5.1 Установление формального процесса 25
3.5.2 Контроль за ходом реализации стратегии 26
3.5.3 Оценка результатов стратегии 26

4 Общие принципы 29
4.1 Концепция 30
4.2 Комплексный подход и установление адаптированных приоритетов 30
4.3 Открытость 31
4.4 Социально-экономическое благополучие 31
4.5 Основные права человека 31
4.6 Управление рисками и способность к восстановлению 32
4.7 Соответствующий набор инструментов политики 33
4.8 Четкое руководство, распределение функций и ресурсов 33
4.9 Доверительная среда 33
5 Передовой опыт разработки национальной стратегии кибербезопасности 35
5.1 Приоритетная область 1. Управление 36
5.1.1 Обеспечение высочайшего уровня поддержки 36
5.1.2 Создание компетентного органа в области кибербезопасности 37
5.1.3 Обеспечение межведомственного сотрудничества 37
5.1.4 Обеспечение межсекторального сотрудничества 38
5.1.5 Выделение специального бюджета и ресурсов 38
5.1.6 Разработка плана реализации 38
5.2 Приоритетная область 2. Управление рисками в области национальной кибербезопасности 39
5.2.1 Оценка киберугроз и согласование политики с постоянно растущим масштабом киберугроз 39
5.2.2. Определение подхода к управлению рисками 39
5.2.3 Определение общей методики управления рисками кибербезопасности 40
5.2.4 Разработка секторальных профилей рисков в области кибербезопасности 40
5.2.5 Разработка политики кибербезопасности 40
5.3 Приоритетная область 3. Подготовленность и способность к восстановлению 41
5.3.1 Создание возможностей реагирования на киберинциденты 41
5.3.2 Разработка планов для непредвиденных ситуаций в целях управления кризисами в сфере кибербезопасности и аварийного восстановления 41
5.3.3 Содействие совместному использованию информации 42
5.3.4 Проведение учений по кибербезопасности 42
5.3.5 Оценка воздействия или серьезности инцидентов кибербезопасности 43
5.4 Приоритетная область 4. Критически важная инфраструктура и основные услуги 43
5.4.1 Разработка подхода к управлению рисками для выявления и защиты критически важной инфраструктуры и основных услуг 44
5.4.2 Принятие модели управления с четко установленными обязанностями 44
5.4.3 Определение минимальных базовых уровней кибербезопасности 45

5.4.4 Использование широкого ряда рыночных рычагов 45
5.4.5 Создание государственно-частных партнерств 46
5.5 Приоритетная область 5. Возможности и создание потенциала, а также повышение осведомленности 46
5.5.1 Стратегическое планирование и наращивание потенциала, повышение осведомленности 46
5.5.2 Разработка учебных программ в области кибербезопасности 47
5.5.3 Стимулирование развития навыков и профессиональной подготовки рабочей силы 47
5.5.4 Реализация программы повышения осведомленности в области кибербезопасности 48
5.5.5 Содействие инновациям и научно-исследовательским и опытно-конструкторским работам в области кибербезопасности 48
5.5.6 Специальные программы для уязвимых секторов и групп 49
5.6 Приоритетная область 6. Законодательство и регулирование 49
5.6.1 Создание внутренней правовой базы по кибербезопасности 49
5.6.2 Создание внутренней правовой базы по киберпреступности и электронным доказательствам 50
5.6.3 Признание и гарантирование прав и свобод личности 50
5.6.4 Создание механизмов обеспечения соблюдения 51
5.6.5 Содействие созданию потенциала для охраны правопорядка 51
5.6.6 Разработка межорганизационных процессов 51
5.6.7 Поддержка международного сотрудничества для борьбы с киберугрозами и киберпреступностью 52
5.7 Приоритетная область 7. Международное сотрудничество 52
5.7.1 Признание кибербезопасности компонентом внешней политики и согласование внутренних и международных усилий 53
5.7.2 Участие в международных дискуссиях и стремление к реализации 53
5.7.3 Содействие официальному и неофициальному сотрудничеству в киберпространстве 54
5.7.4 Содействие наращиванию потенциала для международного сотрудничества 55
6 Справочные материалы 57
Жизненный цикл национальной стратегии кибербезопасности 58
Инициирование 58
Критический обзор и анализ 58
Разработка национальной стратегии кибербезопасности 58
Реализация 59
Контроль и оценка 59
Общие принципы 59
Концепция 59
Комплексный подход и установление адаптированных приоритетов 59
Открытость 60
Социально-экономическое благополучие 60
Основные права человека 60

Управление рисками и способность к восстановлению 61
Соответствующий набор инструментов политики 62
Четкое руководство, распределение функций и ресурсов 62
Доверительная среда 63
Приоритетные области 63
ПО 1. Управление 63
ПО 2. Управление рисками в области национальной кибербезопасности 64
ПО 3. Подготовленность и способность к восстановлению 65
ПО 4. Критически важная инфраструктура и основные услуги 66
ПО 5. Возможности и создание потенциала, а также повышение осведомленности 67
ПО 6. Законодательство и регулирование 68
ПО 7. Международное сотрудничество 69
7 Акронимы 71

Вступление

Руководство по разработке национальной стратегии кибербезопасности является одним из наиболее полных обзоров того, что представляют собой успешные стратегии кибербезопасности. Это результат уникальных равнозначных совместных усилий многих заинтересованных сторон.

Партнеры пришли к единому мнению о необходимости укрепления сотрудничества и координации в рамках международного сообщества в области наращивания потенциала кибербезопасности. Целью этих усилий является поддержка национальных лидеров и директивных органов в разработке защитных и упреждающих мер реагирования на киберриски в форме национальной стратегии кибербезопасности, а также в стратегическом осмыслении вопросов кибербезопасности, киберготовности, реагирования и устойчивости, обеспечения уверенности и безопасности при использовании ИКТ.

Руководство разработано с использованием итеративного подхода, направленного на достижение согласия путем формирования консенсуса. Его основой являются существующие ресурсы и стремление облегчить его использование национальными заинтересованными сторонами. Там, где это возможно, соответствующие источники и инструменты, использовавшиеся для разработки каждого набора рекомендаций, перечислены в разделе "Справочные материалы", чтобы стимулировать их более широкое применение.

Кибербезопасность является основополагающим элементом, лежащим в основе достижения социально-экономических целей современной экономики. Мы надеемся, что это второе издание Руководства по разработке национальной стратегии кибербезопасности сможет и впредь служить полезным инструментом для всех заинтересованных сторон, участвующих в разработке и реализации официальных документов такого типа, включая национальных политиков, законодателей и регуляторные органы, ответственные за обеспечение кибербезопасности в своих странах. Кроме того, оно может получить более широкое применение, так как приведенные в нем концепции можно применять на региональном или муниципальном уровнях, а также адаптировать для промышленности или использовать в научных исследованиях.

Примечание для читателей о внесенных изменениях

Версия 2 Руководства по разработке национальной стратегии кибербезопасности представляет собой обновленный, уточненный и расширенный вариант версии 1, опубликованной в 2018 году. С тех пор проблема киберрисков значительно изменилась и усложнилась, и в данной версии Руководства сделана попытка отразить основные тенденции в области кибербезопасности, которые следует учитывать в национальном стратегическом планировании. Хотя версия 2 Руководства расширяет и улучшает содержание версии 1, в ней не изменены ни структура документа, ни уровень его детализации. Явно выраженной целью этой новой версии была совместимость с версией 1. Внесенные изменения можно резюмировать следующим образом:

- важность целенаправленного финансирования и инвестирования в необходимые ресурсы: использованы более подробные формулировки, чтобы подчеркнуть важность инвестирования в необходимые экономические, людские и организационные ресурсы на протяжении всего жизненного цикла стратегии (разработка, реализация и пересмотр);
- вовлечение заинтересованных сторон: в этой версии еще раз подчеркивается решающая роль частного сектора и гражданского общества в процессах реагирования на инциденты и управления ими, обмена информацией и повышения осведомленности как внутри страны, так и за рубежом. Кроме того, больше внимания уделено той роли в разработке и реализации национальной стратегии кибербезопасности, которую могут играть международные организации. Существует множество международных, неправительственных и многосторонних организаций, специализирующихся на поддержке национальных правительств;
- устойчивость и взаимозависимость: в обновленном тексте подчеркивается важность учета сложности интернет-инфраструктуры страны и возникающих в результате зависимостей и уязвимостей, взаимосвязей и взаимозависимости между секторами, а также других рисков цепочки поставок. Приведена более подробная информация о передовом опыте для поощрения сотрудничества между различными заинтересованными сторонами в целях устранения растущих рисков и повышения устойчивости перед лицом расширяющейся области угроз;
- междисциплинарный подход к наращиванию киберпотенциала: в этой версии Руководства признается, что кибербезопасность применима ко всем вертикалям общества, и даются более подробные рекомендации по разработке инклюзивных и междисциплинарных мероприятий по наращиванию потенциала, включая усилия в области политики, правоохранительной деятельности, образования, осведомленности и дипломатии;
- законодательство, регулирование и права человека: в этой версии более широко представлен передовой опыт в области разработки внутреннего законодательства и регулирования в сфере кибербезопасности и киберпреступности, а также защиты прав и свобод человека;
- международное сотрудничество: в обновленном Руководстве больше внимания уделяется областям, которые стратегия могла бы охватить в части сотрудничества и взаимодействия в сфере кибербезопасности на региональном и международном уровнях, в том числе в рамках международных торговых соглашений, регионального экономического партнерства и добровольных норм ответственного поведения государств в киберпространстве. Подчеркивается важность международного сотрудничества правоохранительных органов и формальных или неформальных механизмов для обмена информацией, укрепления доверия и поддержки трансграничного сотрудничества в борьбе с киберпреступностью и другими преступлениями с использованием кибертехнологий.

Раздел 1

Обзор документа

1.1 Цель

Цель настоящего документа состоит в том, чтобы помочь национальным лидерам и директивным органам в разработке национальной стратегии кибербезопасности, а также в стратегическом осмыслении вопросов кибербезопасности, киберготовности и устойчивости.

Руководство призвано обеспечить полезную, гибкую и удобную для пользователей основу для определения контекста социально-экономического развития страны и текущего положения в области безопасности, а также помочь директивным органам разработать стратегию, учитывающую конкретную ситуацию в стране, ее культурные и социальные ценности и поощряющую стремление к созданию безопасных, устойчивых, основанных на ИКТ и соединенных сообществ.

Руководство является уникальным ресурсом, поскольку оно обеспечивает структуру, согласованную организациями, обладающими подтвержденным и разнообразным опытом в этой области, и основано на их предшествующей работе. Таким образом, это наиболее полный на сегодняшний день обзор того, что представляют собой успешные национальные стратегии кибербезопасности.

1.2 Сфера применения

Кибербезопасность – это комплексная проблема, которая включает несколько различных управленческих, политических, эксплуатационных, технических и правовых аспектов. В этом Руководстве предпринята попытка рассмотреть, систематизировать и расставить приоритеты во многих из этих областей на основе существующих широко признанных моделей, систем и других справочных материалов. Основное внимание в Руководстве уделяется элементам защиты гражданских аспектов киберпространства, и поэтому рассматриваются общие принципы и примеры передового опыта, которые необходимо учитывать в процессе подготовки проекта национальной стратегии кибербезопасности, ее разработки и управления ею.

Для этого в Руководстве проводится четкое различие между "процессом", который будет принят странами во время жизненного цикла национальной стратегии кибербезопасности (инициирование, критический обзор и анализ, создание, реализация, контроль и оценка), и "содержанием", то есть фактическим текстом, который войдет в документ национальной стратегии кибербезопасности. В Руководстве не рассматриваются такие аспекты, как развитие оборонительных или наступательных киберсистем военными структурами, силами обороны или разведывательными службами страны, несмотря на то, что ряд стран разрабатывает такие системы.

В настоящем Руководстве даются указания и рекомендации как относительно того, "что" должно быть включено в национальную стратегию кибербезопасности, так и относительно того, "как" разрабатывать, внедрять и пересматривать такую стратегию.

В Руководстве также представлен обзор базовых компонентов, необходимых странам для того, чтобы они могли стать киберподготовленными, и выделены важные аспекты, которые правительства должны учитывать при разработке своих национальных стратегий и планов реализации.

И наконец, в этом Руководстве представителям директивных органов предлагается всеобъемлющий общий обзор существующих подходов и приложений со ссылкой на дополнительные источники, которые могут быть использованы при реализации конкретных видов деятельности в области кибербезопасности на национальном уровне.

1.3 Общая структура и указания по использованию Руководства

Настоящее Руководство в первую очередь представляет собой ресурс, призванный помочь государственным заинтересованным сторонам в подготовке, разработке национальной стратегии кибербезопасности и управлении ею. Таким образом содержание организовано в соответствии с процессом и порядком разработки стратегии.

- **Раздел 2.** Введение. Содержит обзор предмета Руководства с соответствующими определениями.
- **Раздел 3.** Жизненный цикл разработки стратегии. Подробное описание этапов разработки стратегии и управления ею в течение всего ее жизненного цикла.
- **Раздел 4.** Общие принципы стратегии. Излагаются сквозные фундаментальные соображения, которые необходимо учитывать при разработке стратегии.
- **Раздел 5.** Приоритетные области и примеры передовой практики. Определение ключевых элементов и тем, которые следует рассмотреть при разработке стратегии.
- **Раздел 6.** Вспомогательные справочные материалы. Представлены дополнительные указатели соответствующей литературы, которую заинтересованные стороны могут изучить в рамках своих усилий по составлению проекта стратегии.

В частности, в разделе 3 рассматриваются процесс и аспекты, связанные с разработкой национальной стратегии кибербезопасности (такие как подготовка, разработка, реализация и долгосрочная устойчивость), а в разделах 4 и 5 больше внимания уделяется содержанию национальной стратегии кибербезопасности, поскольку в них освещаются понятия и элементы, которые должен содержать документ.

1.4 Целевая аудитория

Настоящее Руководство предназначено в первую очередь для представителей директивных органов, ответственных за разработку национальной стратегии кибербезопасности. Вторичная аудитория – это все остальные заинтересованные представители государственных и частных организаций, участвующие в разработке и реализации стратегии, например ответственные сотрудники государственных, регуляторных и правоохранительных органов, поставщики услуг ИКТ, операторы критически важной инфраструктуры, представители гражданского общества, академических организаций и научно-исследовательских учреждений. Руководство также может оказаться полезным для различных заинтересованных сторон в международном сообществе в сфере развития, которые оказывают помощь в области кибербезопасности.

Раздел 2

Введение

С момента создания информационно-коммуникационных технологий они превратились в основу современного бизнеса, критически важных услуг и инфраструктуры, социальных сетей и мировой экономики в целом.

В результате руководители государств начали внедрять цифровые стратегии и финансировать проекты, расширяющие возможности подключения к интернету и использующие преимущества, связанные с применением ИКТ, для стимулирования экономического роста, повышения производительности и эффективности, усовершенствования предоставления услуг и возможностей обслуживания, обеспечения доступа к бизнесу и информации, а также для обеспечения возможностей электронного обучения, повышения квалификации рабочей силы и содействия благому управлению. Страны не могут игнорировать преимущества, связанные с возможностью установления соединений и участия в интернет-экономике.

В то время как зависимость нашего общества от цифровой инфраструктуры растет, технологии остаются изначально уязвимыми. Конфиденциальности, целостности и доступности инфраструктуры ИКТ угрожают быстро меняющиеся риски, включая мошенничество с использованием электронных средств, кражу интеллектуальной собственности и информации, позволяющей установить личность, сбои в обслуживании, а также повреждение или уничтожение имущества. Преобразующая сила ИКТ и интернета как катализаторов экономического роста и социального развития находится в критической точке, когда доверие граждан и государств к использованию ИКТ подрывается отсутствием кибербезопасности.

Чтобы полностью реализовать потенциал информационных технологий, государства должны увязать свои национальные экономические концепции с национальными приоритетами в области безопасности. Если риски безопасности, связанные с распространением ИКТ-инфраструктуры и интернет-приложений, не будут должным образом сбалансированы с комплексными национальными стратегиями кибербезопасности и планами обеспечения устойчивости, страны не смогут добиться экономического роста и достичь тех целей национальной безопасности, к которым они стремятся. В ответ страны разрабатывают как наступательные, так и оборонительные возможности, чтобы защитить себя от незаконной злонамеренной деятельности в киберпространстве и упреждать инциденты до того, как они смогут причинить ущерб. В настоящем документе рассмотрены конкретные защитные меры, в частности выраженные в форме национальных стратегий кибербезопасности.

2.1 Что такое кибербезопасность

Существует несколько национальных и международных определений термина "кибербезопасность". Для целей настоящего документа термин "кибербезопасность" используется для описание набора инструментов, правил, руководств, подходов к управлению рисками, действий, учебных курсов, практических рекомендаций, гарантий и технологий, которые могут быть использованы для защиты доступности, целостности и конфиденциальности активов в подключенных инфраструктурах, принадлежащих государственным учреждениям, частным организациям и гражданам; к таким активам относятся подключенные вычислительные устройства, персонал, инфраструктура, приложения, цифровые услуги, системы электросвязи и данные в цифровой среде.

2.2 Преимущества национальной стратегии кибербезопасности и процесс ее разработки

Национальная стратегия кибербезопасности может принимать различные формы с разным уровнем детализации в зависимости от целей и уровня киберготовности конкретной страны. Поэтому устоявшегося и общепринятого определения национальной стратегии кибербезопасности не существует.

Опираясь на проведенные в этой области исследования, авторы настоящего документа предлагают заинтересованным сторонам рассматривать национальную стратегию кибербезопасности:

- как выражение концепции, общих целей, принципов и приоритетов, которыми руководствуется страна в решении проблем кибербезопасности;
- обзор круга заинтересованных сторон, которым поручено повышение уровня кибербезопасности страны, и их соответствующих функций и обязанностей;
- описание шагов, программ и инициатив, которые страна намерена предпринять для защиты своей национальной киберинфраструктуры и для повышения при этом уровня безопасности и устойчивости.

Заблаговременное определение концепции, целей и приоритетов позволяет правительствам комплексно рассматривать кибербезопасность в рамках своей национальной цифровой экосистемы, а не на уровне отдельного сектора экономики, отдельной цели или реакции на конкретный риск – это позволяет им действовать стратегически. Приоритеты национальной стратегии кибербезопасности различаются в зависимости от страны, поэтому в одной стране основное внимание может уделяться устранению рисков, связанных с критически важной инфраструктурой, а в другой это может быть защита интеллектуальной собственности, укрепление доверия к онлайн-среде или повышение осведомленности широкой публики в вопросах кибербезопасности или сочетание этих задач.

Необходимость выявить и впоследствии определить приоритетность соответствующих инвестиций и ресурсов имеет решающее значение для успешного управления рисками в такой всеобъемлющей области, как обеспечение кибербезопасности.

Национальная стратегия кибербезопасности также создает возможности для согласования приоритетов в области кибербезопасности с другими задачами, связанными с ИКТ. Кибербезопасность имеет решающее значение для достижения социально-экономических целей современной экономики, и стратегия должна отражать то, как она обеспечивается. Это можно сделать, проанализировав существующую политику, направленную на реализацию цифровых программ страны или программ развития, или оценив способы включения вопросов кибербезопасность в такие программы.

Наконец, в процессе разработки национальной стратегии кибербезопасности концепция правительства должна быть преобразована в последовательную и осуществимую политику, помогающую ему достичь своих целей. Это включает в себя не только меры, программы и инициативы, которые необходимо выполнить, но и ресурсы, выделенные для этих усилий, а также способы использования этих ресурсов. Также в ходе этого процесса должны также быть определены показатели, которые будут использоваться для достижения желаемых результатов в рамках установленных бюджетов и сроков.

Раздел 3

Жизненный цикл национальной стратегии кибербезопасности

Данный раздел содержит обзор различных этапов разработки стратегии. Это следующие этапы:

- Этап I. Инициирование
- Этап II. Критический обзор и анализ
- Этап III. Разработка национальной стратегии кибербезопасности
- Этап IV. Реализация
- Этап V. Контроль и оценка

В этом разделе также представлены ключевые структуры, которые должны быть привлечены к разработке стратегии, и указаны другие соответствующие заинтересованные стороны, которые могут внести вклад в этот процесс.

В конечном итоге цель этого раздела – дать читателю представление о шагах, которые должна предпринять страна для разработки национальной стратегии кибербезопасности, и о возможных механизмах реализации этой стратегии в соответствии с конкретными нуждами и потребностями страны, с учетом общих принципов (описанных в разделе 4) и примеров передовой практики (описанных в разделе 5).

Как показано на рисунке 1, этот жизненный цикл помогает читателям настоящего документа сосредоточиться на стратегическом осмыслении кибербезопасности на национальном уровне.

3.1 Этап I. Инициирование

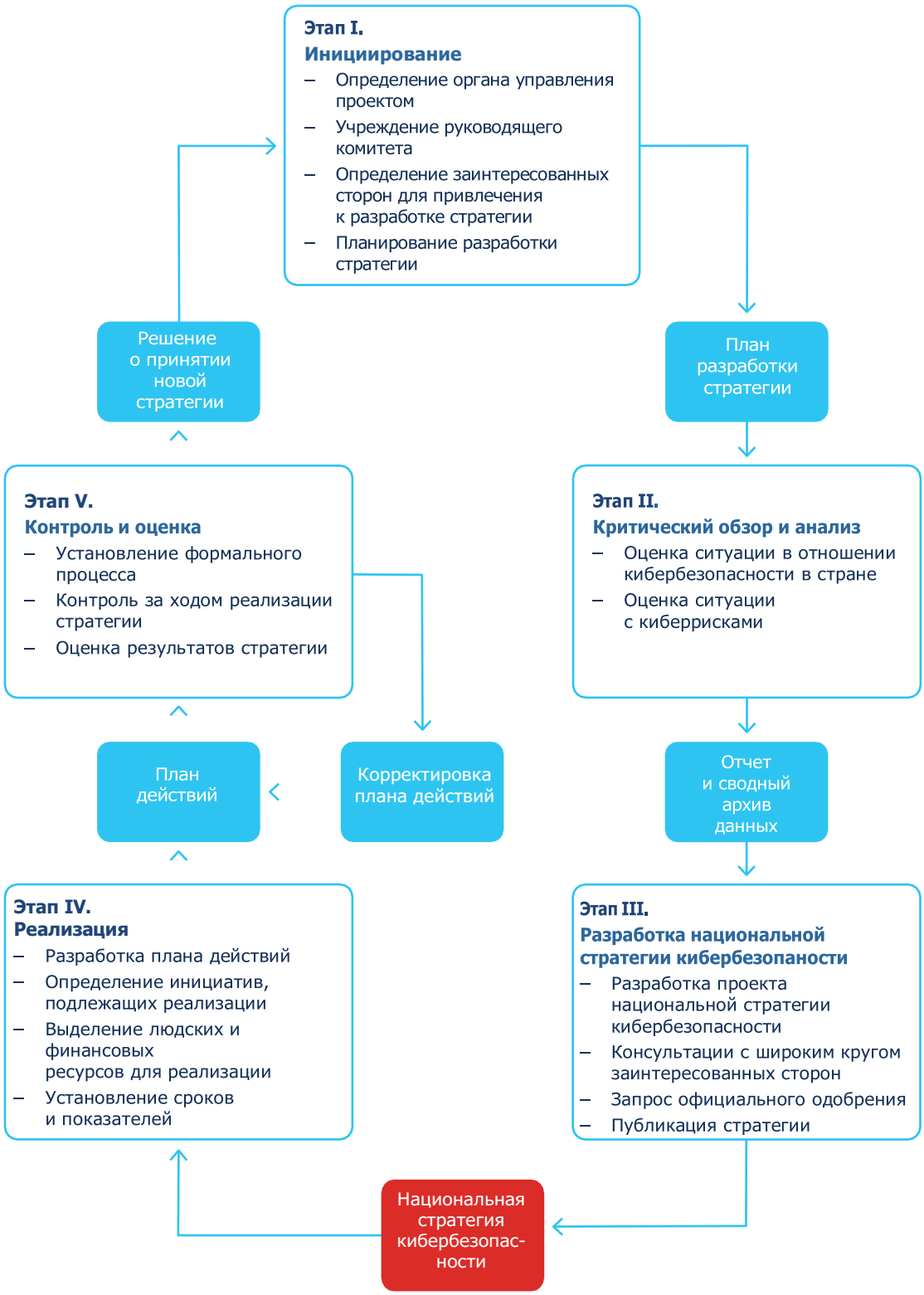
Как указано в разделах 4 и 5 настоящего документа, этап инициирования национальной стратегии кибербезопасности обеспечивает основу для ее эффективной разработки. Предполагается, что на этом этапе основное внимание будет уделено процессам, срокам и определению ключевых заинтересованных сторон, которые должны быть привлечены к разработке стратегии. Результатом этого этапа является план разработки стратегии. Если это предусмотрено процессом государственного управления, может потребоваться, чтобы этот план был одобрен исполнительной властью.

3.1.1 Определение органа управления проектом

В соответствии с принципом четкого определения руководства, распределения функций и ресурсов (раздел 4.8) процесс разработки стратегии должен координироваться единым компетентным органом. Для руководства разработкой стратегии орган исполнительной власти должен назначить существующую или вновь созданную государственную структуру, такую как министерство, ведомство или департамент. Эта структура, именуемая в настоящем документе органом управления проектом, в свою очередь должна назначить лицо или группу лиц, ответственных за руководство процессом разработки стратегии.

Орган управления проектом должен оставаться нейтральным на протяжении всего процесса разработки. Поэтому рекомендуется, чтобы эта организация отличалась от той, которая отвечает за реализацию стратегии. Должны быть приняты те или иные механизмы, чтобы преодолеть предвзятость и избежать внутриведомственную конкуренцию за ресурсы.

Рисунок 1. Жизненный цикл национальной стратегии кибербезопасности

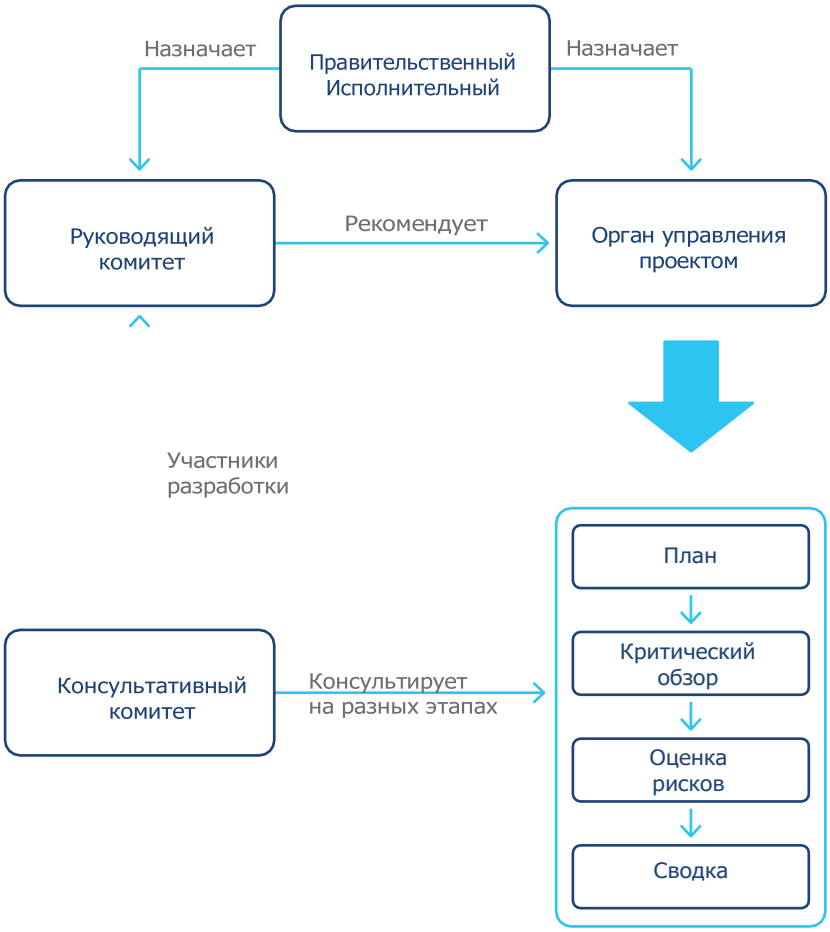


3.1.2 Учреждение руководящего комитета

Исполнительный орган также должен создать руководящий комитет для работы с органом управления проектом в процессе разработки стратегии. Он должен быть уполномочен давать руководящие указания, а также выполнять определенные функции в обеспечении качества. Кроме того, он должен гарантировать прозрачность и открытость процесса в соответствии с принципом четкого руководства и распределения функций и ресурсов (раздел 4.8). Функции руководящего комитета, его структура и членский состав должны быть четко определены с самого начала.

Поскольку может потребоваться, чтобы руководящий комитет рассматривал конфиденциальные документы, он должен быть сформирован соответствующим образом. Также важно, чтобы его членский состав отражал различные обязанности, возложенные на этот орган, например посредством старшинства назначений.

Рисунок 2. Заинтересованные стороны



3.1.3 Определение заинтересованных сторон для привлечения к разработке стратегии

На этом этапе орган управления проектом должен определить первоначальную группу заинтересованных сторон, которых необходимо привлечь к разработке стратегии. Ему также следует уточнить функции этих заинтересованных сторон и наметить способы их сотрудничества для управления ожиданиями на протяжении всего процесса.

В течение процесса органу управления проектом может потребоваться привлечь дополнительные заинтересованные стороны, чтобы использовать все имеющиеся знания и опыт. Это касается принципа открытости (раздел 4.3), который подчеркивает важность сотрудничества с целым рядом заинтересованных сторон из правительства, частного сектора и гражданского общества. Например, орган управления проектом может рассмотреть возможность привлечения к участию ИКТ-компаний, операторов критически важной инфраструктуры, ученых и представителей неправительственных организаций, работающих над повышением уровня осведомленности и готовности в области кибербезопасности, и т. д.

Для такого механизма сотрудничества орган управления проектом может создать консультативный комитет, который мог бы способствовать назначению членов для работы в руководящем комитете, а также проводить консультации на различных этапах разработки стратегии. По возможности его состав должен быть достаточно широким и включать представителей от всех секторов общества, которые могут оказаться под влиянием стратегии.

Кроме того, орган управления проектом по рекомендации руководящего комитета мог бы рассмотреть возможность привлечения международных заинтересованных сторон, чтобы получить дополнительную поддержку или экспертные знания. Существует целый ряд международных, неправительственных и частных организаций, специализирующихся на поддержке национальных правительств в их деятельности в области разработки национальных стратегий кибербезопасности (NCS).

3.1.4 Определение людских и финансовых ресурсов

На этом этапе орган управления проектом должен определить людские и финансовые ресурсы, необходимые для разработки и реализации стратегии, а также источники, из которых их можно получить. Например, необходимые экспертные знания можно запросить у межправительственных организаций, компаний частного сектора, гражданского общества, научных учреждений или агентств по развитию. Аналогичным образом потребности в финансировании могут быть удовлетворены за счет перераспределения целевых потоков финансирования в рамках существующих бюджетов или за счет нового внешнего финансирования (например, от международных организаций).

Особое внимание следует уделить обеспечению долгосрочного финансирования всего жизненного цикла национальной стратегии кибербезопасности, включая ее разработку, реализацию и совершенствование. Дополнительные сведения о выделении ресурсов для реализации стратегии см. в разделе "Выделение людских и финансовых ресурсов для реализации стратегии" (раздел 3.4.3), а дополнительные сведения о долгосрочном финансировании – в разделе "Выделение специального бюджета и ресурсов" (раздел 5.1.5).

3.1.5 Планирование разработки стратегии

На заключительном шаге этапа инициирования орган управления проектом должен подготовить план разработки национальной стратегии кибербезопасности. После составления плана его надлежащим образом представляют на утверждение руководящему комитету и исполнительному органу в соответствии с процессами государственного управления.

При составлении плана органу управления проектом также следует рассмотреть вопрос о том, примет ли национальная стратегия кибербезопасности форму законодательства или политики, поскольку различные варианты могут повлиять на формальные процессы, которым необходимо следовать, а также на сроки принятия стратегии.

В плане разработки стратегии должны быть определены основные этапы и мероприятия, ключевые заинтересованные стороны, сроки и потребности в ресурсах, в том числе людских и финансовых. В нем должно быть указано, как и когда соответствующие заинтересованные стороны будут участвовать в процессе разработки, чтобы внести свой вклад и установить обратную связь.

Возможные варианты взаимодействия и распределение функций между заинтересованными сторонами и комитетами показаны на рисунке 2.

Дополнительные источники информации перечислены на с. 58.

3.2 Этап II. Критический обзор и анализ

Цель этого этапа заключается в сборе данных для оценки ситуации в стране в области кибербезопасности и существующих и будущих киберрисков. Эта оценка необходима как источник информации для составления проекта и разработки национальной стратегии кибербезопасности. Итогом этого мероприятия, проведенного консультативным комитетом или при его содействии, должен стать отчет, содержащий обзор общей ситуации в стране в области стратегии и рисков кибербезопасности, который будет представлен руководящему комитету.

Прежде чем приступить к фактическому составлению (или пересмотру) текста стратегии, орган управления проектом должен тщательно проанализировать и оценить информацию, собранную на этапе критического обзора, чтобы убедиться, что выявлены любые пробелы в потенциале кибербезопасности и представлены варианты их устранения. Результатом анализа должна стать оценка того, насколько существующая политика, регуляторная и операционная среда соответствуют выявленным потребностям страны, а также выявление тех областей, где они не соответствуют требованиям.

Этот этап также следует использовать для выявления конкретных ключевых проблем, таких как пробелы в образовании и профессиональной подготовке.

Наконец, анализ должен привести к оценке всех соответствующих и желаемых результатов стратегии, а также необходимых и доступных средств, которые могут быть использованы для достижения желаемых целей.

3.2.1 Оценка общей ситуации в стране в области кибербезопасности

Для того чтобы национальная стратегия кибербезопасности была эффективной, она должна отражать ситуацию с кибербезопасностью в стране. С этой целью следует провести анализ существующих сильных и слабых сторон кибербезопасности в стране, а также ознакомиться с соответствующими материалами и документами в сотрудничестве с соответствующими заинтересованными сторонами из правительства, частного сектора и гражданского общества. На этом этапе должен быть применен принцип комплексного подхода и адаптированных приоритетов (описанный в разделе 4.2). Орган управления проектом при поддержке консультативного комитета также должен оценить функции и обязанности различных заинтересованных сторон в системе государственной кибербезопасности, чтобы распространить эффективные практики и сократить дублирование

В рамках этих усилий орган управления проектом должен определить ресурсы и службы, критически важные для правильного функционирования общества и экономики, и провести обзор существующих национальных законов, нормативных актов, правил, программ и возможностей, связанных с кибербезопасностью. Орган управления проектом также должен выявить существующие механизмы мягкого регулирования, такие как государственно-частное партнерство, и оценить созданные возможности для решения проблем кибербезопасности, такие как национальные группы экстренного реагирования, группы реагирования на компьютерные инциденты или группы реагирования на инциденты компьютерной безопасности (CERT/CIRT/CSIRT). Кроме того, следует определить и сопоставить функции и обязанности существующих государственных ведомств, наделенных полномочиями в области кибербезопасности, таких как регуляторные органы или агентства по защите данных.

В дополнение к этому следует собрать соответствующие данные, которые могут быть использованы для оценки состояния кибербезопасности в стране. Это может быть информация о существующих национальных программах кибербезопасности; международных инициативах; многосторонних и двусторонних соглашениях; проектах частного сектора; программах в области ИКТ, киберобразования и повышения квалификации; инициативах в области НИОКР, связанных с кибербезопасностью; данные о проникновении и заражении интернета, внедрении ИКТ и технологических разработках; а также предположения относительно будущих тенденций и угроз в области ИКТ и кибербезопасности.

В этот анализ также следует включить соответствующую информацию, предоставленную частным сектором, научно-исследовательскими институтами и другими группами заинтересованных сторон. Для развивающихся стран также крайне важно наметить совместные с партнерами инициативы по развитию для координации технической помощи и инвестиций.

Наконец, органу управления проектом следует изучить аналогичную информацию на региональном и международном уровнях и отраслевые стратегии и инициативы.

3.2.2 Оценка ситуации с киберрисками

Основываясь на информации, собранной на предыдущем этапе, орган управления проектом должен оценить риски, с которыми сталкивается страна из-за цифровой зависимости. Это можно сделать путем выявления национальных цифровых активов, как государственных, так и частных, взаимозависимостей между ними, уязвимостей и угроз, а также путем оценки вероятности и потенциального влияния инцидентов кибербезопасности.

Эти усилия связаны с принципом управления рисками и способности к восстановлению (раздел 4.6), согласно которому управление рисками имеет решающее значение для полной реализации преимуществ цифровой среды в целях социально-экономического развития. Кроме того, эта первоначальная оценка рисков может стать основой для будущих, более конкретных оценок рисков (дополнительная информация о принципе управления рисками и способности к восстановлению и о способах проведения оценки рисков содержится в разделе 5.2).

Дополнительные источники информации приведены на с. 58.

3.3 Этап III. Разработка национальной стратегии кибербезопасности

Целью этого этапа является разработка текста стратегии путем привлечения основных заинтересованных сторон из государственного сектора, частного сектора и гражданского общества в рамках серии публичных консультаций и рабочих групп. Эта расширенная группа заинтересованных сторон, координируемая органом управления проектом, будет отвечать за определение общей концепции и сферы применения стратегии, формулирование общих целей, оценку текущей ситуации (которая детализируется на этапе II), определение приоритетов в отношении воздействия на общество, граждан и экономику, а также за обеспечение необходимых финансовых ресурсов. В рамках этого этапа следует рассмотреть все сквозные принципы (раздел 4) и элементы передовой практики (раздел 5), подробно описанные в настоящем Руководстве.

3.3.1 Разработка проекта национальной стратегии кибербезопасности

По завершении этапа критического обзора и анализа орган управления проектом в сотрудничестве с руководящим комитетом инициирует разработку стратегии. Могут быть созданы специальные рабочие группы для работы над конкретными темами или для разработки различных разделов стратегии. Эти рабочие группы должны следовать процессам, установленным на этапе инициирования разработки, корректируя их по мере необходимости.

В стратегии должно быть определено общее направление обеспечения кибербезопасности в стране; представлены четкая концепция и сфера применения; установлены цели, которые должны быть достигнуты в определенные сроки; и определена их приоритетность с точки зрения воздействия на общество, экономику и инфраструктуру. Более того, она должна определять возможные направления деятельности, стимулировать усилия по реализации и побуждать к выделению необходимых ресурсов для поддержки всех этих мероприятий. Стратегия может также включать некоторые выводы, сделанные на этапе критического обзора и анализа.

Как и на этапе планирования разработки стратегии, в соответствующем документе должна быть представлена четкая структура управления (раздел 5.1), определяющая функции и обязанности основных заинтересованных сторон. Сюда относится определение органа, ответственного за управление стратегией и ее оценку, а также органа, ответственного за общее управление и реализацию, такого как центральный руководящий орган или национальный совет по кибербезопасности.

Стратегия также должна определять или подтверждать полномочия различных структур, участвующих в национальной архитектуре кибербезопасности страны, в том числе ответственных за инициирование и разработку политики и правил кибербезопасности; сбор информации об угрозах и уязвимостях; реагирование на инциденты кибербезопасности (например, национальные группы CERT/CIRT/CSIRT); а также за повышение уровня готовности и обеспечение кризисного управления. В ней также должно быть четко определено, как все эти организации взаимодействуют друг с другом и с центральным руководящим органом.

3.3.2 Консультации с широким кругом заинтересованных сторон национального, регионального и международного уровней

Как упоминалось выше, решающее значение для успеха стратегии имеет привлечение заинтересованных сторон. Для того чтобы окончательный вариант стратегии основывался на общей концепции, проект документа следует распространить среди широкого круга заинтересованных сторон, не ограничиваясь участниками процесса разработки стратегии. Это можно сделать посредством проведения различных мероприятий, таких как онлайн-консультации, семинары по проверке и дополнительные рабочие группы. Международные организации и другие внешние заинтересованные стороны могут сыграть определенную роль на этапе консультаций, давая советы и предоставляя экспертные знания. Предполагается, что отзывы и комментарии, полученные в результате этого процесса, будут использованы для окончательной доработки стратегии.

3.3.3 Запрос официального одобрения

На заключительном этапе разработки стратегии орган управления проектом должен обеспечить официальное принятие стратегии органом исполнительной власти. Этот официальный процесс принятия может варьироваться в зависимости от страны и основывается на том, как стратегия определена в законодательной базе. Например, она может приниматься посредством парламентской процедуры или постановлением правительства.

Кроме того, крайне важно, чтобы стратегия не только разрабатывалась с одобрения на самом высоком уровне, но чтобы эта приверженность сохранялась на этапе ее реализации. Соответствующие должностные лица должны нести ответственность и пользоваться поддержкой как в виде политического капитала, так и в виде ресурсов.

3.3.4 Публикация и продвижение стратегии

Стратегия должна быть публичным легкодоступным документом. В идеале выпуск стратегии должен сопровождаться внутренними и внешними мероприятиями по ее продвижению. Широкая доступность стратегии гарантирует, что общественность будет осведомлена о приоритетах и целях правительства в области кибербезопасности, и поддержит любые усилия по повышению осведомленности по вопросам кибербезопасности. Если стратегия сопровождается планом действий, то в последнем также должны быть указаны дополнительные возможности для дальнейшего взаимодействия и сотрудничества с гражданским обществом, частным сектором и международными партнерами.

Дополнительные источники информации приведены на с. 58.

3.4 Этап IV. Реализация

Этап реализации, вероятно, является наиболее важным элементом всего жизненного цикла национальной стратегии кибербезопасности. Структурированный подход к реализации, подкрепленный надлежащими людскими и финансовыми ресурсами, имеет решающее значение для успеха стратегии и должен рассматриваться как часть ее разработки. Основной составляющей этапа реализации часто является план действий, который определяет различные запланированные мероприятия.

3.4.1 Разработка плана действий

Как и в случае разработки стратегии, ее реализация не может быть исключительной ответственностью одного органа. Она требует участия и координации различных заинтересованных сторон в правительстве, а также поддержки со стороны гражданского общества и частного сектора. Эффективной реализации стратегии может способствовать план действий, разработанный в соответствии с принципом четкого руководства, распределения функций и выделения ресурсов (раздел 4.8).

Разработка плана действий почти так же важна, как сам план. Процесс, организуемый органом управления проектом, должен служить механизмом объединения соответствующих заинтересованных сторон для согласования задач и результатов, а также для координации усилий и объединения ресурсов.

3.4.2 Определение инициатив, которые необходимо реализовать

Национальная стратегия кибербезопасности высвечивает цели правительства и результаты, которых оно стремится достичь в определенных приоритетных областях. В плане действий орган управления проектом – в координации с соответствующими заинтересованными сторонами – определяет конкретные инициативы, которые помогут достичь этих целей в каждой приоритетной области. Примерами таких инициатив могут служить, в частности, организация учений по кибербезопасности, установление базовых показателей безопасности для критически важных инфраструктур и создание системы отчетности об инцидентах.

Сроки и усилия, необходимые для реализации этих инициатив, должны быть расставлены по приоритетам в соответствии с их важностью, чтобы обеспечить надлежащее использование ограниченных ресурсов. С этой целью можно рассмотреть результаты и итоги этапа II (критический обзор и анализ), особенно в отношении "Оценки ситуации с киберрисками" (раздел 3.2.2).

3.4.3 Выделение людских и финансовых ресурсов для реализации стратегии

После определения приоритетных инициатив орган управления проектом должен назначить конкретные государственные структуры в качестве ответственных за реализацию каждой из этих инициатив. В свою очередь эти государственные структуры будут нести ответственность за реализацию каждой конкретной порученной им инициативы и, как ожидается, будут координировать свои усилия с другими заинтересованными сторонами в рамках процесса реализации.

Чтобы гарантировать, что эти структуры смогут достичь ожидаемых результатов, орган управления проектом должен оценить, был ли им выдан соответствующий мандат – юридический или иной, – необходимый для реализации стратегии. Орган управления проектом также должен сотрудничать с организациями, ответственными за реализацию конкретных инициатив, чтобы понять, какие ресурсы потребуются им для выполнения работ. Эта оценка должна учитывать потребности в людских ресурсах, экспертных знаниях и финансировании. Затем орган управления проектом работает с ответственными организациями, помогая им определить необходимые ресурсы и обеспечить их в соответствии с административно-финансовыми структурами страны.

3.4.4 Установление сроков и показателей

Последним критически важным элементом плана действий является разработка конкретных параметров и ключевых показателей эффективности (КПЭ) для оценки каждой из предпринятых инициатив, например чтобы убедиться, что в стране проведена информационная кампания относительно важности обмена информацией, организована и выполнена программа учений по кибербезопасности в секторе критически важной инфраструктуры или что принят основополагающий закон о безопасности. Также должны быть установлены конкретные сроки реализации.

Орган управления проектом разрабатывает параметры и ключевые показатели эффективности в партнерстве с соответствующими операторами. Последних следует поощрять к определению и использованию более подробного набора показателей для облегчения оценки эффективности и действенности инициатив во время и после их завершения.

Дополнительные источники информации приведены на с. 59.

3.5 Этап V. Контроль и оценка

Разработка и реализация стратегии – это непрерывный процесс. Компетентный орган должен разработать официальный процесс контроля и оценки стратегии. На этапе контроля правительство должно гарантировать, что стратегия реализуется в соответствии с планом действий. На этапе оценки правительство и национальный компетентный орган оценивают, является ли стратегия по-прежнему актуальной и подходящей в свете меняющейся ситуации с рисками, по-прежнему ли она отражает цели руководства страны и необходимы ли какие-либо корректировки.

3.5.1 Установление формального процесса

Для обеспечения эффективности контроля и оценки реализации стратегии правительству необходимо назначить независимый орган, ответственный за контроль и оценку хода реализации и его эффективности. В идеале этот орган должен участвовать в определении соответствующих показателей контроля и оценки в отношении реализации стратегии и связанного с ней плана действий и инициатив, что имеет место на этапах разработки и инициирования.

Контроль и измерение эффективности и успешного выполнения плана реализации стратегии должны быть частью существующих в стране механизмов управления. Непрерывная оценка плана реализации (то есть того, что идет хорошо, а что нет) помогает совершенствовать стратегию. Механизмы надлежащего управления в отношении реализации стратегии также должны четко определять подотчетность и ответственность за обеспечение успешного выполнения. Установление параметров или КПЭ по краткосрочным, среднесрочным и долгосрочным целям помогает укрепить механизмы руководства и управления. Ключевые показатели эффективности или параметры должны отвечать требованиям SMARRT.

- **Конкретность** (**Specific**) – определите конкретную область для улучшения и сосредоточьтесь на ожидаемых изменениях.
- **Измеримость** (**Measurable**) – дайте количественную оценку или, по крайней мере, предложите показатель прогресса.
- **Достижимость** (**Achievable**) – укажите, каких результатов реально достичь при имеющихся ресурсах.
- **Релевантность** (**Relevant**) – сосредоточьтесь на значимых показателях прогресса.
- **Привязка к исполнителю** (**Responsible**) – укажите, кто будет это делать.
- **Привязка к сроку** (**Time-related**) – укажите, когда можно достичь результата(ов).

Установление базовых показателей позволит лучше контролировать действия и выявлять области для потенциального улучшения. Кроме того, распределение бюджетов должно соответствовать уровню амбиций и сложности желаемого эффекта.

3.5.2 Контроль за ходом реализации стратегии

Орган, ответственный за контроль за ходом реализации стратегии, должен осуществлять это в соответствии с согласованным графиком в течение всего жизненного цикла стратегии. Любые отклонения от согласованных сроков и причины любых задержек, такие как изменение приоритетов, нехватка персонала или ресурсов и т. д., отражаются в итоговом документе (например, в отчете). Это следует делать в дополнение к периодическим отчетам, которые организации, ответственные за различные направления реализации стратегии, представляют органу управления проектом. В процессе контроля за реализацией стратегии должны активно участвовать все соответствующие заинтересованные стороны.

Такой подход гарантирует ответственность соответствующих заинтересованных сторон за выполнение взятых на себя обязательств; это также обеспечит раннее выявление любых проблем, связанных с реализацией. Это в свою очередь позволит правительству исправить ситуацию или соответствующим образом скорректировать свои планы на основе уроков, извлеченных в процессе реализации стратегии.

3.5.3 Оценка результатов стратегии

В дополнение к оценке прогресса по согласованным показателям важно также периодически оценивать результаты и сравнивать их с первоначально поставленными целями. Это имеет решающее значение для понимания того, достигаются ли цели стратегии или следует рассмотреть возможность принятия других мер.

В рамках этого процесса также необходимо регулярно пересматривать более широкую ситуацию с рисками, чтобы понять, влияют ли какие-либо внешние изменения на результаты стратегии. По сути этот процесс представляет собой простой пересмотр профиля оценки рисков страны.

Оценка вместе с соответствующими рекомендациями включается в отчет для органа управления проектом и должна указывать способы пересмотра плана действий и обеспечения его актуальности и соответствия меняющимся политике и ситуации с рисками.

В конечном итоге отчеты, подготовленные в течение жизненного цикла стратегии, должны стать основой для общего обзора национальной стратегии кибербезопасности в соответствии с графиком, установленным на этапе инициирования. В этом общем обзоре должны быть учтены не только достигнутый прогресс и изменения внешней ситуации, но и пересмотр собственных приоритетов и целей правительства.

Дополнительные источники информации приведены на с. 59.

Раздел 4

Общие принципы

В этом разделе приведены девять основополагающих принципов, которые в комплексе могут помочь в разработке перспективной и целостной национальной стратегии кибербезопасности.

Эти принципы применимы ко всем ключевым областям деятельности, рассматриваемым в данном документе. Их следует учитывать на всех этапах процесса разработки национальной стратегии кибербезопасности – от составления проекта стратегии до ее реализации.

Порядок изложения этих принципов отражает их логическую связь, а не степень важности.

4.1 Концепция

Стратегия должна отражать четкую концепцию, принятую как государством, так и обществом

Стратегия с большей вероятностью будет успешной в том случае, если она определяет концепцию, которая помогает всем заинтересованным сторонам понять, что поставлено на карту и почему эта стратегия необходима (контекст), что должно быть достигнуто (цели), а также в чем она состоит и на кого оказывает влияние (сфера применения).

Чем четче эта концепция, тем легче будет руководителям и ключевым заинтересованным сторонам принять комплексный, согласованный и последовательный подход. Четкая концепция облегчает также процесс координации, сотрудничества и реализации стратегии с участием соответствующих заинтересованных сторон. Эта концепция должна быть сформулирована на достаточно высоком уровне и учитывать динамичный характер цифровой среды.

С этой концепцией должны быть согласованы цели и сроки реализации стратегии.

Дополнительные источники информации приведены на с. 59.

4.2 Комплексный подход и установление адаптированных приоритетов

Стратегия должна стать результатом всестороннего осмысления и анализа общей цифровой среды и в то же время учитывать особые обстоятельства и приоритеты страны

Кибербезопасность – это не только техническая задача, но и сложный и многогранный вопрос, аспекты которого выходят далеко за рамки социально-экономического благополучия и затрагивают такие области, как обеспечение соблюдения законов, национальная и международная безопасность, международные отношения, торговые переговоры и устойчивое развитие.

Важно понимать все аспекты кибербезопасности, а также то, как они взаимосвязаны между собой, потенциально дополняя друг друга или конкурируя друг с другом. На основе такого осмысления и анализа конкретных условий страны в дальнейшем могут быть определены приоритеты в соответствии с целями и сроками реализации стратегии. Эти приоритеты позволят поставить конкретные задачи, установить сроки и выделить необходимые ресурсы.

Приоритеты, включенные в национальную стратегию кибербезопасности, будут разными в разных странах. Некоторые из вопросов кибербезопасности могут рассматриваться в одном и том же или в отдельных стратегических документах (например, цифровые аспекты национальной безопасности и обороны могут рассматриваться в рамках национальной стратегии в области безопасности или обороны).

Дополнительные источники информации приведены на с. 59.

4.3 Открытость

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

Цифровая среда стала критически важной для правительств, организаций и отдельных лиц. Эти группы сталкиваются с рисками кибербезопасности и несут определенную ответственность за управление ими в зависимости от их функций и обязанностей. По этой причине правительствам рекомендуется установить партнерские отношения и механизмы сотрудничества, чтобы привлечь частный сектор и гражданское общество к обсуждению киберстратегии и процесса ее реализации.

Хотя это может быть и непростая задача, но для разработки и успешной реализации национальной стратегии кибербезопасности необходимо определить и привлечь все соответствующие заинтересованные стороны. Это поможет понять потребности заинтересованных сторон и использовать их уникальные знания и опыт, содействуя тем самым сотрудничеству для достижения целей стратегии.

Чтобы обеспечить открытость и прозрачность, стратегия должна быть общедоступным документом. Дополнительные источники информации приведены на с. 60.

4.4 Социально-экономическое благополучие

Стратегия должна содействовать обеспечению социально-экономического благополучия и максимально возможного вклада ИКТ в устойчивое развитие и социальную интеграцию

Цифровая среда способна ускорить экономический рост и социальный прогресс, способствовать реализации основных ценностей общества, усовершенствовать предоставление государственных услуг, содействовать развитию международной торговли и надлежащему государственному управлению.

Все более широкое использование цифровой среды для удовлетворения потребностей общества повысило внимание к вопросам кибербезопасности. Однако обеспечение кибербезопасности не является самоцелью. Стратегия должна быть увязана с более широкими социально-экономическими целями и способствовать формированию доверия и уверенности, необходимых как для содействия достижению этих целей, так и для защиты страны от киберугроз.

Дополнительные источники информации приведены на с. 60.

4.5 Основные права человека

Стратегия должна уважать основные права человека и соответствовать им

В стратегии должно признаваться, что права, которые человек имеет в офлайновой среде, должны быть защищены также и в онлайновой среде. Она должна уважать общепризнанные основные права человека, в том числе права, закрепленные во Всеобщей декларации прав человека и Международном пакте о гражданских и политических правах Организации Объединенных Наций, а также в соответствующих многосторонних или региональных правовых документах.

Внимание должно быть уделено свободе выражения мнений, конфиденциальности сообщений и защите персональных данных. В частности, стратегия должна не допускать содействия практике произвольного, неоправданного или иного незаконного наблюдения, перехвата сообщений или обработки персональных данных.

Гарантируя государству возможность принимать меры для удовлетворения своих законных интересов и в то же время уважая права человека отдельных лиц, стратегия должна обеспечить, чтобы, когда это применимо, наблюдение, перехват сообщений и сбор данных осуществлялись в контексте специального расследования или судебного дела, санкционированного соответствующим органом государственной власти, или на основе открытой, конкретной, всеобъемлющей и недискриминационной нормативно-правовой базы, позволяющей осуществлять эффективный надзор и обеспечивающей процессуальные гарантии и права.

Дополнительные источники информации приведены на с. 60.

4.6 Управление рисками и способность к восстановлению

Стратегия должна обеспечивать эффективное управление рисками кибербезопасности и укреплять способность к восстановлению экономической и социальной деятельности

Хотя цифровая среда предоставляет заинтересованным сторонам экономические и социальные возможности, она в то же время подвергает их рискам кибербезопасности. Например, когда организации используют ИКТ для содействия инновациям, повышения производительности и конкурентоспособности или когда правительства развертывают свои услуги в онлайновой среде, могут возникать инциденты, связанные с кибербезопасностью, способные привести к финансовым потерям, ущербу для репутации, нарушению операций, физическим воздействиям, подрыву инноваций и т. д. Как и в случае с другими типами риска, риски кибербезопасности не могут быть полностью устранены, однако ими можно управлять и свести к минимуму.

Чтобы решить эту проблему, стратегия должна побуждать предприятия вкладывать средства в первую очередь в кибербезопасность и активно управлять рисками. В тех случаях, когда предприятия готовы идти на риск ради получения прибыли, необходимо поддерживать баланс между мерами безопасности и потенциально возможными выгодами, учитывая динамичный характер цифровой среды. Стратегия также должна признавать необходимость постоянного управления рисками и содействовать использованию согласованного подхода взаимозависимыми структурами.

Заинтересованные стороны, которые уделяют внимание управлению рисками, будут подготовлены к возможным инцидентам, связанным с нарушением безопасности, обеспечивая тем самым устойчивость социально-экономической деятельности в стране. Именно поэтому стратегия должна поощрять принятие мер по обеспечению непрерывности деятельности и восстановлению после бедствий, которые включают управление инцидентами и кризисными ситуациями, а также планы восстановления.

Дополнительные источники информации приведены на с. 61.

4.7 Соответствующий набор инструментов политики

Стратегия должна использовать наиболее подходящие из имеющихся инструментов политики для достижения каждой из ее целей, учитывая конкретные обстоятельства, сложившиеся в соответствующей стране

Цели правительства в области кибербезопасности будут достигнуты только в том случае, если в поведении всех заинтересованных сторон произойдут изменения. В большинстве случаев правительства имеют в своем распоряжении различные рычаги и инструменты политики для достижения этих результатов. Они включают, в частности, законодательство, регулирование, стандартизацию, сертификацию, стимулирование, программные элементы и механизмы обмена информацией, образовательные программы, обмен передовым опытом, установление желательных норм поведения и формирование сообществ доверия. Каждый из этих механизмов имеет свои сильные и слабые стороны, требует различных затрат и приносит различные результаты.

Наилучшие результаты могут быть достигнуты путем выбора наиболее подходящего инструмента политики для каждой отдельной цели и сбалансированного использования различных инструментов.

Дополнительные источники информации приведены на с. 62.

4.8 Четкое руководство, распределение функций и ресурсов

Стратегия должна быть принята на самом высоком уровне правительства, которое затем будет нести ответственность за распределение соответствующих функций и обязанностей, а также за выделение достаточных людских и финансовых ресурсов

Кибербезопасность должна находить поддержку и содействие на самых высоких уровнях управления. Кроме того, чтобы обеспечить подотчетность и прогресс, необходимо определить координаторов отдельных направлений работы, а все участвующие стороны должны иметь четкое представление о своих соответствующих функциях и обязанностях. Стратегия должна также предусматривать выделение людских, финансовых и материальных ресурсов, необходимых для ее реализации. Этот принцип должен направлять как процесс разработки стратегии, так и разработку плана действий для этой стратегии.

Дополнительные источники информации приведены на с. 62.

4.9 Доверительная среда

Стратегия должна помочь создать цифровую среду, которой граждане и предприятия могли бы доверять

Укрепление доверия в национальной цифровой экосистеме, в которой права и интересы пользователей защищены, а безопасность данных и систем гарантирована, имеет важнейшее значение для реализации всех потенциальных социальных, политических и экономических возможностей, связанных с использованием ИКТ. Стратегия должна создать условия для реализации мер политики, процессов и различных видов деятельности на национальном уровне, чтобы сделать безопасным предоставление важнейших услуг (включая, помимо прочего, электронное правительство, электронную коммерцию и цифровые финансовые транзакции) на основе ИКТ, которыми пользуются граждане. Это позволило бы укоренить принцип доверия не только среди широких слоев населения, но и среди государственных и частных организаций, которые будут предлагать гражданам свои услуги ИКТ.

Дополнительные источники информации приведены на с. 63.

Раздел 5

Передовой опыт разработки национальной стратегии кибербезопасности

Кибербезопасность затрагивает многие области социально-экономического развития и зависит от ряда факторов, обусловленных национальным контекстом.

В связи с этим в данном разделе представлен набор элементов передового опыта, которые могут сделать стратегию всеобъемлющей и эффективной и в то же время позволяют адаптировать ее к национальному контексту.

Эти элементы передового опыта сгруппированы по приоритетным областям – общим темам национальной стратегии кибербезопасности. Хотя здесь в качестве примеров передовой практики представлены как приоритетные области, так и элементы передового опыта, важно, чтобы последние рассматривались в национальном контексте, поскольку некоторые из них могут не соответствовать конкретной ситуации в стране. Страны должны выявлять элементы передового опыта, которые способствуют выполнению их задач и достижению приоритетов в соответствии с концепцией, установленной в их стратегии (раздел 4), и следовать им. Порядок представления отдельных элементов или приоритетных областей, приведенный ниже, не следует рассматривать как указание на степень важности или приоритетности.

5.1 Приоритетная область 1. Управление

К этой приоритетной области относятся элементы передового опыта, которые следует рассмотреть на предмет включения в текст стратегии при разработке структуры управления национальной кибербезопасностью (включая все организации, наделенные обязанностями и полномочиями для развития цифровой экономики и снижения рисков, связанных с кибернебезопасностью). В стратегии должны быть четко указаны цели и результаты, которые правительство ставит перед страной, чтобы повысить ее устойчивость и снизить риски для ее компаний, критически важных инфраструктур, услуг и активов. В стратегии должны быть четко определены функции и обязанности заинтересованных сторон, которым поручено ее реализация, и предусмотрены меры по привлечению органов власти и должностных лиц к ответственности за реализацию, контроль, оценку и результаты выполнения стратегии (см. *"Жизненный цикл национальной стратегии кибербезопасности"*).

С этой целью в стратегии следует определить и наделить полномочиями компетентный орган, ответственный за выполнение стратегии; создать механизм для определения государственных структур, затрагиваемых стратегией или ответственных за ее реализацию, и поставить перед ними соответствующие задачи; включить в план реализации стратегии конкретные цели – измеримые, достижимые, ориентированные на результат и намеченные на конкретные сроки; а также признать необходимость выделения ресурсов (политической воли, финансирования, времени, людских ресурсов и т. д.) для достижения желаемых результатов.

5.1.1 Обеспечение высочайшего уровня поддержки

Стратегия должна получить официальное одобрение на самом высоком уровне государственного управления. Это одобрение служит двум важным целям. Во-первых, оно повышает вероятность того, что будут выделены достаточные ресурсы и что усилия по координации окажутся успешными. Во-вторых, оно сигнализирует более широкой национальной экосистеме о том, что кибербезопасность страны неразрывно связана с ее цифровой экономикой и другими социально-политическими аспектами, зависящими от цифровых систем, и должна быть национальным приоритетом.

Возможно, также потребуется законодательно закрепить стратегию во внутренней нормативно-правовой базе, чтобы придать ей правомочность и приоритет в национальном масштабе.

5.1.2 Создание компетентного органа в области кибербезопасности

В стратегии должен быть определен специальный национальный компетентный орган, ответственный за реализацию стратегии. Это должен быть руководитель (физическое лицо или организация) высокого ранга, имеющий прочные позиции на самом высоком правительственном уровне, способный обеспечить руководство, координацию действий и контроль за реализацией стратегии. Компетентный орган также несет ответственность за отчетность о ходе и результатах реализации стратегии.

Такой национальный компетентный орган также должен действовать в качестве органа управления, который определяет и уточняет функции, обязанности, процессы, права принятия решений и задач, необходимых для обеспечения эффективной реализации стратегии. Сюда относятся определение заинтересованных сторон, которые будут осуществлять надзор за реализацией стратегии, и установление целевых показателей эффективности для различных министерств или ведомств, учреждений и отдельных лиц, ответственных за конкретные аспекты стратегии и последующего плана действий. В некоторых случаях положение национального компетентного органа в области кибербезопасности, возможно, будет необходимо закрепить в политике или законе, чтобы наделить его полномочиями для выполнения поставленных перед ним задач.

Учитывая тот факт, что кибербезопасность затрагивает множество различных областей, важно гарантировать, что компетентный государственный орган имеет возможность привлекать и направлять соответствующие заинтересованные стороны. Для этого также может потребоваться дополнительное законодательство, обязывающее государственные учреждения отчитываться перед национальным компетентным органом о своем прогрессе в достижении целей стратегии в измеримых показателях. Эффективным способом оценки прогресса является использование ключевых показателей эффективности (КПЭ).

5.1.3 Обеспечение межведомственного сотрудничества

В стратегии должен быть установлен механизм определения и привлечения государственных структур, затрагиваемых при ее реализации или ответственных за нее. Приверженность, координация и сотрудничество в рамках правительства являются основными функциями этих государственных учреждений, гарантирующими, что механизмы управления (стандарты, правила, рыночные стимулы и т. д.) и ресурсы принесут желаемые результаты при реализации стратегии. Наличие хорошо зарекомендовавшего себя национального компетентного органа высокого уровня в области кибербезопасности также поможет улучшить внутриправительственную координацию и сотрудничество.

Эффективная связь и координация гарантируют, что все министерства и ведомства будут осведомлены о соответствующих полномочиях, задачах и целях друг друга. Приверженность, в свою очередь, заключается в поддержке последовательной долгосрочной политики для выполнения обещаний, содержащихся в стратегии. Примером механизма координации может служить проведение периодических совещаний всех соответствующих заинтересованных сторон, участвующих в планах действий, подлежащих совместному рассмотрению. Примером механизма сотрудничества может служить создание межведомственной целевой группы для решения конкретного вопроса. Примером приверженности являются согласованные программы внутренней и внешней политики

страны, чтобы одно министерство не подрывало доверие к другому, выражая разные позиции по одной и той же политической проблеме (например, торговые потоки противопоставляются экспортному контролю технологий двойного назначения).

5.1.4 Обеспечение межсекторального сотрудничества

Стратегия должна отражать понимание зависимости правительства от частного сектора и других неправительственных заинтересованных сторон в стране (и наоборот) в деле создания надежной, безопасной и устойчивой экосистемы (принцип открытости). С этой целью в стратегии следует четко указать, как правительство будет взаимодействовать с этими различными заинтересованными сторонами, и определить их функции и обязанности. Например, в стратегии должна быть определена сеть авторитетных координаторов в критически важных отраслях, необходимых для обеспечения функционирования и восстановления критически важных услуг и инфраструктуры.

Стратегия должна быть согласована с другими национальными приоритетами, такими как обеспечение возможности установления приемлемых в ценовом отношении доступных соединений для всех; повышение уровня защиты данных и конфиденциальности при одновременном содействии инновациям; повышение устойчивости инфраструктуры и доступности услуг в условиях стихийных бедствий, изменения климата и пандемий; изучение новых технологий, таких как ИИ, блокчейн, квантовые вычисления и т. д. (принцип 2 *"Комплексный подход и установление адаптированных приоритетов"*).

5.1.5 Выделение специального бюджета и ресурсов

В стратегии должно быть оговорено выделение надлежащих специальных ресурсов для ее реализации, поддержания и пересмотра. Достаточное, последовательное и бесперебойное финансирование составляет основу эффективной национальной системы кибербезопасности.

Должны быть определены финансовые ресурсы (то есть выделен бюджет), а также людские и материально-технические ресурсы. Для успешной реализации также требуются политическая приверженность и лидерство, подкрепленные надежным партнерством. Цели и задачи в рамках стратегии не следует рассматривать как одноразовое выделение ресурсов. Потребности в ресурсах необходимо регулярно пересматривать в зависимости от прогресса или недостатков в реализации целей и задач стратегии.

Правительство может также рассмотреть вопрос о создании централизованного бюджета расходов на кибербезопасность, управляемого центральным механизмом управления кибербезопасностью. Независимо от того, будут ли разрозненные источники финансирования объединены в согласованную комплексную программу или создан единый внутригосударственный бюджет, для обеспечения успешной реализации стратегии необходима общая программа, которая должна управляться и отслеживаться по этапам.

5.1.6 Разработка плана реализации

Стратегия должна сопровождаться планом реализации или ссылаться на план, в котором подробно описан процесс достижения ее стратегических целей. В эффективном плане реализации должны быть указаны подотчетные организации, ответственные за каждую задачу и цель, ресурсы, которые потребуются для их выполнения с течением времени (в краткосрочной, среднесрочной и долгосрочной перспективе), используемые процессы и ожидаемые результаты (см. раздел 3.4 о начале реализации).

Дополнительные источники информации приведены на с. 63.

5.2 Приоритетная область 2. Управление рисками в области национальной кибербезопасности

В этой приоритетной области представлены примеры передовой практики обеспечения кибербезопасности посредством управления рисками. В соответствии с принципом управления рисками и способностью к восстановлению (раздел 4.6), следует применять подход управления рисками, поскольку полностью устранить киберриски невозможно. Осознание страной рисков, которым она подвержена, помогает ей более эффективно управлять ими. Подход к оценке риска должен быть сосредоточен на выявлении взаимозависимостей и учитывать риски, возникающие в результате трансграничных зависимостей. Подход к управлению рисками должен учитывать весь жизненный цикл от разработки или закупки до эксплуатации и замены.

Также важно отметить, что поскольку угрозы кибербезопасности чрезвычайно динамичны и непредсказуемы, любой подход к управлению рисками следует регулярно пересматривать. Таким образом, для обеспечения постоянного усовершенствования стратегия должна предусматривать контроль и оценку деятельности по управлению рисками.

5.2.1 Оценка киберугроз и согласование политики с постоянно растущим масштабом киберугроз

Стратегия должна определять и оценивать меняющуюся ситуацию с киберугрозами, а также их потенциальное влияние и последствия для критически важных инфраструктур и основных услуг. Стратегия должна в первую очередь определять внутренние критически важные инфраструктуры и службы – физические и кибернетические системы и ресурсы, жизненно важные для надлежащего функционирования общества и экономики, выход из строя или разрушение которых окажет пагубное воздействие на физическую или экономическую безопасность или на общественное здравоохранение или защищенность страны.

Необходимо провести оценку ситуации с киберугрозами, чтобы выявить конкретные киберугрозы и риски для критически важных инфраструктур и служб, а также лиц, которые их используют и полагаются на них, и определить приоритетность выделения ресурсов для их защиты. Такая оценка также могла бы служить основой для согласования стратегии управления киберрисками с планом кризисного управления страны. Она также поможет использовать необходимые возможности, людские ресурсы, финансирование и стратегии для укрепления общего состояния национальной кибербезопасности.

5.2.2. Определение подхода к управлению рисками

Стратегия должна определять согласованный подход к управлению рисками, которому должны следовать все государственные структуры и операторы критически важной инфраструктуры в стране.

Этот подход должен быть направлен на разработку оценки киберугроз и создание национального реестра рисков, который должен надежно храниться и передаваться, позволяя правительству осуществлять надзор за рисками и методами управления ими. Кроме того, в рамках этого подход следует разработать метод определения приоритетов, основанный на расчете вероятности реализации рисков и их последствий. Кроме того, должны быть указаны обязанности ключевых подразделений в каждом секторе в отношении оценки, принятия и предотвращения рисков кибербезопасности на национальном уровне.

5.2.3 Определение общей методики управления рисками кибербезопасности

Стратегия должна определять общую методику управления рисками кибербезопасности. Это обеспечит эффективность и согласованность по всем организациям и облегчит обмен информацией об угрозах и рисках между взаимозависимыми системами. Следует отдавать предпочтение методике, основанной на международных стандартах, поскольку она может снизить затраты и улучшить взаимодействие с частным сектором.

Методика должна обеспечивать рекомендации по распределению функций и обязанностей по различным аспектам управления рисками, таким как оценка угроз, оценка ресурсов, внедрение и поддержание мер по смягчению последствий и принятие остаточного риска. Методика должна включать программу сертификации, помогающую оценить и в конечном итоге повысить уровень соответствия.

Важно отметить, что в отношении закупки и разработки инфраструктуры или услуг методика управления рисками должна содержать рекомендации по минимизации рисков с помощью безопасного проектирования архитектуры и регулярных оценок/проверок, признавая, что безопасность лучше всего достигается, когда она является неотъемлемой частью процесса проектирования, разработки и внедрения продукта, технологического процесса или услуги (безопасность по замыслу).

5.2.4 Разработка секторальных профилей рисков в области кибербезопасности

Стратегия должна предусматривать использование отраслевых профилей риска в области кибербезопасности. Отраслевой профиль риска представляет собой количественный анализ типов угроз, с которыми сталкивается отрасль. Цель профиля риска – обеспечить менее субъективное понимание риска путем присвоения числовых значений переменным, представляющим разные типы угроз и степени их опасности. Стратегия должна рекомендовать разработку профилей риска для тех отраслей, которые страна считает наиболее важными для своего общества и экономики. (Эти отраслевые профили риска могут быть частью процесса оценки ситуации с киберугрозами, описанного в разделе 5.2.1.)

Использование отраслевых профилей риска обеспечивает основу для более конкретных оценок риска для отдельных организаций, гарантирует согласованность внутри всех отраслей национальной экономики и между ними и сокращает ресурсы, необходимые для оценки организационных рисков. Их следует регулярно обновлять, чтобы они оставались актуальными.

5.2.5 Разработка политики кибербезопасности

Стратегия должна содействовать разработке политики кибербезопасности для важнейших национальных организаций, таких как органы государственного управления, операторы критически важных инфраструктур и др. Такая политика, принятая согласно принципу соответствующего набора инструментов политики (раздел 4.7), должна охватывать управленческие, эксплуатационные и технические требования и инструктировать заинтересованные стороны в отношении их функций и обязанностей, а также направлять или предписывать конкретные подходы к решению этих вопросов.

Например, такая политика может касаться кибербезопасности при закупках или разработке, определять программы обмена информацией, координировать раскрытие уязвимостей, устанавливать минимальные стандарты осторожности, определять базовые уровни безопасности, регламентировать программы сертификации на соответствие требованиям и предписывать передачу информации об инцидентах кибербезопасности компетентным органам.

Скоординированный подход на национальном уровне может привести к более эффективному и действенному управлению кибербезопасностью, поскольку будет гармонизировать практику и облегчит координацию и функциональную совместимость.

Дополнительные источники информации приведены на с. 64.

5.3 Приоритетная область 3. Подготовленность и способность к восстановлению

В рамках этой приоритетной области представлен обзор передовой практики, которая поддерживает создание и устойчивость эффективных национальных возможностей для подготовки к серьезным инцидентам в области кибербезопасности, их предотвращения, обнаружения, смягчения последствий и реагирования на них, а также для повышения общей киберустойчивости страны.

5.3.1 Создание возможностей реагирования на киберинциденты

Стратегия должна содействовать созданию соответствующих национальных возможностей реагирования на инциденты для решения оперативных проблем кибербезопасности. Нередко это означает создание групп реагирования на нарушения компьютерной защиты (CERT), групп реагирования на компьютерные инциденты (CSIRT) или групп реагирования на инциденты компьютерной безопасности (CIRT) с общенациональным уровнем ответственности.

Хотя конкретные организационные формы групп CERT/CSIRT/CIRT могут варьироваться (национальные, государственные, отраслевые и т. д.) и потребности и ресурсы стран могут различаться, эти специализированные целевые группы должны предпринимать как упреждающие действия, так и действия по реагированию на инциденты, а также выполнять профилактические и образовательные функции. Таким образом, эти организации могут повысить способность страны к быстрому реагированию и восстановлению после кибератак, а также ее устойчивость к киберугрозам, снижая возможные общие экономические и эксплуатационные последствия кибератак общенационального масштаба.

К числу услуг, которые могут предложить группы CERT/CSIRT/CIRT, относятся реагирование на киберинциденты и координация принимаемых мер, управление уязвимостями, обеспечение осведомленности о ситуации, передача знаний, а также обмен информацией об угрозах и оперативными данными. Стратегия может также содействовать созданию групп PSIRT (группы реагирования на инциденты, связанные с безопасностью продуктов) для повышения способности предприятий частного сектора справляться с уязвимостями ИКТ-продуктов.

В стратегии также должны быть определены и разработаны механизмы сотрудничества и коммуникации между национальными и отраслевыми группами реагирования на инциденты (если они существуют), а также с международными партнерами.

5.3.2 Разработка планов для непредвиденных ситуаций в целях управления кризисами в сфере кибербезопасности и аварийного восстановления

Стратегия должна предусматривать разработку национального плана действий на случай чрезвычайных ситуаций и кризисов в сфере кибербезопасности. План должен входить в состав общего национального плана действий в чрезвычайных ситуациях или быть согласован с ним. Следует также рассмотреть возможность составления конкретного плана для критически важных информационных инфраструктур.

Этот национальный план действий в чрезвычайных ситуациях в сфере кибербезопасности должен учитывать результаты общенациональных оценок рисков и любые межотраслевые зависимости, которые могут повлиять на непрерывность работы критически важных инфраструктур, а также любые механизмы аварийного восстановления. Кроме того, в нем должен быть представлен обзор национальных механизмов реагирования на инциденты, а также определено, как классифицируются инциденты кибербезопасности и как меняется их категория в зависимости от уровня воздействия на критически важные ресурсы и услуги.

5.3.3 Содействие совместному использованию информации

Стратегия должна способствовать созданию механизмов обмена информацией, позволяющих организациям государственного и частного секторов обмениваться актуальными оперативными данными и информацией об угрозах.

Официальные и неофициальные программы обмена информацией могут способствовать эффективной координации и последовательному, точному и надлежащему обмену информацией в ходе мероприятий по реагированию на инциденты и восстановлению; содействовать быстрому обмену информацией об угрозах и оперативными данными между затронутыми и другими заинтересованными сторонами; помочь понять, какие секторы подверглись атакам и атакам какого рода; распространять информацию о возможных методах защиты и смягчения ущерба для затронутых ресурсов; и в конечном счете уменьшить уязвимость и подверженность угрозам вместе с сопутствующими рисками.

В стратегии должна быть определена одна или несколько государственных структур (компетентных органов), ответственных за передачу точной и полезной информации национальному сообществу кибербезопасности, включая организации государственного и частного секторов.

Обмен информацией должен представлять собой двусторонний процесс. Готовность органов государственной власти делиться имеющейся у них информацией демонстрирует структурам частного сектора, что правительство действительно является партнером по обмену информацией об угрозах и его действия могут гарантировать, что сотрудники служб реагирования будут заниматься основными угрозами и будут лучше подготовлены к ним.

5.3.4 Проведение учений по кибербезопасности

Стратегия должна поощрять организацию и координацию внутренних и международных учений по кибербезопасности и реагированию на инциденты. Они могут иметь разный формат (моделирование или учения в режиме реального времени) и предназначаться для технической или нетехнической аудитории.

Учения по кибербезопасности и другие механизмы кризисного планирования могут помочь стране повысить организационный потенциал для эффективного реагирования на инциденты, протестировать процедуры кризисного управления и механизмы связи, проверить операционную способность групп CERT/CSIRT/CIRT к реагированию на инциденты кибербезопасности и перебои в обслуживании в стрессовой ситуации и выявить любые межотраслевые зависимости.

Аналогичным образом международные учения по кибербезопасности помогут повысить потенциал реагирования на киберинциденты участвующих стран, определить транснациональные зависимости, укрепить уверенность и доверие между странами и повысить общий уровень международной устойчивости и готовности.

5.3.5 Оценка воздействия или серьезности инцидентов кибербезопасности

Стратегия должна способствовать созданию механизмов оценки воздействия или серьезности инцидентов кибербезопасности в зависимости от их влияния на критически важные активы, службы, инфраструктуру и людей. Такие оценки необходимы для понимания более широкого контекста инцидента кибербезопасности, включая его потенциальное и фактическое воздействие на различные отрасли и/или группы населения, а также вызываемые им каскадные эффекты.

Эти оценки должны проводиться открыто и прозрачно с проведением консультаций с широким кругом заинтересованных сторон. Они включаются в национальные планы аварийного восстановления и действий в чрезвычайных ситуациях, а результаты этих оценок используются при реагировании на киберинциденты.

Дополнительные источники информации приведены на с. 65.

5.4 Приоритетная область 4. Критически важная инфраструктура и основные услуги

В рамках этой приоритетной области изучаются примеры передовой практики, относящейся к выявлению и защите критически важных инфраструктур (КИ) и критически важных информационных инфраструктур (КИИ), а также к повышению их способности к восстановлению. Стратегия должна признавать и разъяснять важность повышения уровня безопасности и бесперебойной работы КИ и КИИ. Возможные последствия инцидента, влияющего на КИ или КИИ, могут приводить к нарушению общественного порядка, предоставления основных услуг и экономического благополучия страны, и в стратегии следует подчеркнуть важность усилий по управлению киберрисками, направленных на снижение вероятности таких опасных или разрушительных киберинцидентов.

Хотя общепризнанных определений терминов КИ и КИИ не существует и правительствам необходимо решить, какие структуры и службы следует к ним отнести, исходя из своей собственной оценки национальных рисков, для целей настоящего Руководства эти термины определяются следующим образом:

- критически важные инфраструктуры (КИ) – это активы, которые необходимы для функционирования и обеспечения безопасности общества и экономики в данной стране;
- критически важные информационные инфраструктуры (КИИ) – это ИТ- и ИКТ-системы, выполняющие ключевые функции критически важной инфраструктуры страны.

Следует принять во внимание, что концепция основных услуг применима и к услугам, необходимым для поддержания критически важной общественной или экономической деятельности.

В любом случае в число примеров таких КИ, КИИ или основных услуг входят энергетика (электроэнергия, нефть и газ), транспорт (воздушный, железнодорожный, водный и автомобильный), финансы и банковское дело (кредитные учреждения, торговые площадки и центральные контрагенты), здравоохранение (организации здравоохранения, включая больницы, частные клиники и научно-исследовательские институты), коммунальные услуги (водоснабжение и канализация), цифровые технологии и электросвязь (услуги фиксированной и подвижной телефонной связи и доступа к интернет-инфраструктуре, такие как точки обмена интернет-трафиком (IXP), служба доменных имен (DNS) и др.). В конечном счете определения и условные обозначения зависят от геополитических, экономических и культурных особенностей национального контекста.

5.4.1 Разработка подхода к управлению рисками для выявления и защиты критически важной инфраструктуры и основных услуг

В стратегии должна быть подчеркнута важность защиты КИ и КИИ от рисков, связанных с кибербезопасностью, и рекомендован комплексный подход к управлению рисками в соответствии с принципом управления рисками и способностью к восстановлению (раздел 4.6).

Детальная оценка рисков должна служить руководством для выявления национальных КИ, КИИ и основных услуг, нарушение которых может оказать серьезное влияние на здоровье, безопасность, защищенность или экономическое благополучие граждан или на эффективное функционирование правительства или экономики. Стратегия должна включать или сопровождаться списком конкретных КИ и/или КИИ и их взаимосвязей, который по мере необходимости может периодически пересматриваться и обновляться.

Хотя существует множество различных методик определения КИ и КИИ, страны могут рассмотреть возможность применения отраслевых или функциональных критериев, таких как зависимости и взаимозависимости с другой инфраструктурой, службой и областью воздействия, а также важность инфраструктуры для поддержания минимального уровня предоставления услуг. В этом процессе определения и рассмотрения стратегия должна предусматривать заблаговременное и постоянное участие всех заинтересованных сторон, включая органы государственной власти, полугосударственные органы и/или частных операторов инфраструктуры.

Кроме того, для выявления и определения приоритетности реализации программ, а также политических и практических мер, направленных на защиту и укрепление безопасности и способности к восстановлению КИ и КИИ, следует принять подход, основанный на оценке риска. Эти программы и политика должны быть структурированы таким образом, чтобы КИ и КИИ соответствовали общему базовому уровню мер безопасности при сохранении достаточной гибкости, чтобы соответствовать своим собственным оценкам рисков и приоритетам управления рисками. Чтобы использовать существующие передовые методы, обеспечить возможность интеграции отечественной промышленности в глобальные цепочки поставок ИКТ и избежать проблем функциональной совместимости КИ/КИИ при пересечении национальных границ, можно рассмотреть подход к управлению рисками, основанный на хорошо зарекомендовавших себя международных стандартах.

5.4.2 Принятие модели управления с четко установленными обязанностями

Стратегия должна в общих чертах описывать структуру управления, функции и обязанности заинтересованных сторон в отношении защиты КИ и КИИ. В соответствии с принципом четкого руководства, распределения функций и ресурсов (раздел 4.8) для эффективной и действенной программы защиты КИ требуется, чтобы заинтересованные стороны имели четко определенные функции и обязанности и создали механизм координации для управления решением текущих задач.

КИ и КИИ часто не принадлежат государству и не контролируются им, а усилия по защите КИ и КИИ, как правило, превышают возможности и полномочия любого отдельного правительственного ведомства. Поэтому назначение общего координатора по (кибер)безопасности КИ и КИИ, такого как межведомственный комитет, может значительно помочь в усилиях по защите критически важной инфраструктуры.

Модель управления для защиты КИ и КИИ должна включать назначение государственных структур, отвечающих за конкретные отрасли, определение обязанностей и подотчетности операторов КИ и КИИ, а также каналов связи и механизмов сотрудничества между государственными и частными организациями для обеспечения функционирования и восстановления критически важных услуг и инфраструктуры.

Модель управления должна включать механизмы, обеспечивающие координацию и согласованность действий между государственными структурами с совпадающими функциями. Управление также должно гарантировать создание отраслевыми регуляторными органами четких и последовательных требований безопасности, которые позволяют избежать дублирования задач и упорядочить важные усилия по соблюдению требований как государственными, так и частными структурами.

5.4.3 Определение минимальных базовых уровней кибербезопасности

В стратегии должны быть либо указаны существующие, либо должна быть предложена разработка новых законодательных и нормативных актов, определяющих, в частности, минимальные базовые уровни кибербезопасности для операторов КИ и КИИ. Базовые уровни безопасности должны учитывать ряд общих приоритетов управления рисками, а также более конкретные методы обеспечения кибербезопасности, такие как выявление киберрисков и создание структур управления рисками; защита данных и систем с помощью протоколов управления доступом и других мер; контроль цифровой среды и обнаружение потенциальных аномалий или событий; а также реагирование на инциденты и восстановление после них. При разработке таких базовых уровней следует учитывать признанные на международном уровне стандарты и передовой опыт, чтобы обеспечить лучшие результаты и большую эффективность в области безопасности. В качестве отправной точки следует разработать базовые показатели для разных секторов, что позволит повысить совместимость и согласованность отраслевых практик и упростить соблюдение межотраслевых функций.

В стратегии также должно быть подчеркнуто, что базовые уровни кибербезопасности должны быть ориентированы на конечный результат, чтобы обеспечить большую гибкость с течением времени, поскольку ситуация с рисками и технологии продолжают быстро изменяться. Устанавливая цели, к которым должны стремиться организации (например, "контроль логического доступа к критически важным ресурсам"), а не конкретные способы обеспечения безопасности (например, "использовать двухфакторную аутентификацию"), государство и отрасли смогут получать выгоду от постоянного повышения уровня безопасности. Кроме того, основанный на результатах подход к разработке этих базовых уровней может быть дополнен руководством по реализации для конкретной отрасли или практическим руководством, содержащим варианты учета и интеграции практики предприятий.

В дополнение к решению ряда общих приоритетных задач управления рисками базовые уровни кибербезопасности должны также включать требования к закупкам, гарантирующие наличие у поставщиков ИКТ адекватных и контролируемых мер безопасности.

Стратегия должна поддерживать создание устойчивой национальной среды КИ и КИИ и подготавливать заинтересованные стороны к реагированию на инциденты кибербезопасности, смягчению их последствий и последующему восстановлению. Подход к управлению рисками должен поощрять внедрение процессов антикризисного управления, мер по обеспечению непрерывности бизнеса и планов восстановления.

5.4.4 Использование широкого ряда рыночных рычагов

Стратегия должна предусматривать широкий спектр правил, гарантирующих, что все организации и физические лица действительно заинтересованы в выполнении своих индивидуальных обязанностей в области кибербезопасности, соизмеримых с рисками, с которыми они сталкиваются, в соответствии с принципом комплексного подхода и установления адаптированных приоритетов (раздел 4.2).

Выявление разрывов между тем, что могут и должны регулировать рынки, и тем, что требует ситуация с рисками, – важный шаг на пути к определению времени и способов применения ряда стимулов и сдерживающих факторов для повышения уровня безопасности. Для поощрения применения стандартов и методов обеспечения кибербезопасности в КИ и КИИ в стратегии должно быть указано, что правительство рассмотрит ряд вариантов политики и рыночных рычагов, имеющихся в его распоряжении.

5.4.5 Создание государственно-частных партнерств

Стратегия должна содействовать созданию формальных государственно-частных партнерств для повышения безопасности КИ и КИИ. Государственно-частные партнерства – это основа эффективной защиты критически важной инфраструктуры и управления рисками безопасности как в краткосрочной, так и в долгосрочной перспективе. Они необходимы для укрепления доверия между промышленностью и правительством.

Однако для установления устойчивых партнерских отношений необходимо, чтобы все заинтересованные стороны четко понимали цели партнерства и взаимные выгоды в области безопасности, которые вытекают из совместной работы. В число областей партнерства могут входить разработка межотраслевых и конкретных отраслевых базовых уровней кибербезопасности, создание эффективных координационных структур и процессов и протоколов обмена информацией, укрепление доверия, выявление и обмен идеями, подходами и передовым опытом для повышения уровня безопасности, а также улучшение международной координации.

Дополнительные источники информации приведены на с. 66.

5.5 Приоритетная область 5. Возможности и создание потенциала, а также повышение осведомленности

При рассмотрении вопросов кибербезопасности технологические и политические соображения могут доминировать в ущерб фундаментальному человеческому фактору, лежащему в ее основе. В рамках этой приоритетной области рассматриваются проблемы, связанные с наращиванием потенциала кибербезопасности (как человеческого, так и институционального) и повышением осведомленности заинтересованных сторон, включая государственные структуры, граждан, предприятия и другие организации, имеющие решающее значение для развития цифровой экономики страны.

Передовой опыт, рассматриваемый в этом разделе, охватывает вопросы координации деятельности по наращиванию потенциала, создания специальных учебных программ по кибербезопасности и программ повышения осведомленности, расширения программ подготовки и повышения квалификации персонала, принятия международных схем сертификации и поощрения научно-исследовательских и опытно-конструкторских работ (НИОКР).

5.5.1 Стратегическое планирование и наращивание потенциала, повышение осведомленности

В стратегии должны быть четко определены функции и обязанности структур, которым поручено координировать мероприятия по наращиванию потенциала и повышению осведомленности на национальном уровне, чтобы обеспечить рациональное использование ресурсов, отсутствие дублирования усилий и установление подотчетности. Назначенные национальные органы также должны отвечать за осуществление контроля за реализацией и оценкой результатов этой деятельности и при необходимости рекомендовать внесение изменений.

Возможности по обеспечению кибербезопасности, а также наращивание потенциала и повышение осведомленности должны основываться на фактических данных и стратегически планироваться. Детальная оценка ситуации в области национальной кибербезопасности и текущих инициатив по наращиванию потенциала поможет выявить неудовлетворенные потребности в отношении потенциала, навыков и осведомленности, а также станет основой для принятия перспективных решений. Ввиду различий внутри стран и регионов и между ними универсального подхода к определению возможностей в области кибербезопасности и наращивания потенциала не существует, поэтому собранную информацию следует использовать для разработки подходов, адаптированных к конкретному политическому, экономическому и социальному контексту. Ответственные органы могут также разработать план действий, включающий бюджетные ассигнования, сроки и показатели для отслеживания хода выполнения каждого из этих запланированных мероприятий.

5.5.2 Разработка учебных программ в области кибербезопасности

Стратегия должна способствовать разработке или расширению специализированных школьных программ, направленных на ускорение развития навыков кибербезопасности и повышение осведомленности о них в системе формального образования. Учебные программы должны быть меж- или мультидисциплинарными и охватывать как технические, так и нетехнические навыки и темы кибербезопасности, такие как цифровая грамотность, государственная политика, право, управление, экономика, управление рисками, этика, социальные науки и международные отношения. Следует разработать специальные учебные программы по кибербезопасности для начальных и средних школ, ввести курсы по кибербезопасности во все учебные программы по информатике и информационным технологиям в высших учебных заведениях, а также ввести специальные степени и программы стажировки по кибербезопасности.

Учитывая мультидисциплинарный характер образования в области кибербезопасности, следует поощрять университеты, колледжи и другие образовательные учреждения к обеспечению сотрудничества своих отделений и других учебных заведений для оптимизации ресурсов и усилий при разработке или обновлении учебных программ. Эти учреждения могут играть решающую роль в обучении гражданских и военных специалистов уникальным принципам кибербезопасности и служить инкубаторами для будущих кадров, объединяя теорию с методикой преподавания, инструментами и реализацией, а также оптимизируя общеуниверситетские ресурсы для объединения знаний, интеллектуальных способностей и практических навыков.

Учебные программы должны также повышать осведомленность и стимулировать интерес к карьерному росту в области кибербезопасности. Для наращивания усилий в этой области правительству также следует рассмотреть возможность введения различных схем стимулирования, таких как стипендии в рамках частных образовательных программ и гранты для соответствующей стажировки.

5.5.3 Стимулирование развития навыков и профессиональной подготовки рабочей силы

Стратегия должна поощрять разработку программ обучения и развития навыков в области кибербезопасности для специалистов и неспециалистов как в государственном, так и в частном секторах. Эти усилия могут включать в себя подготовку руководящих и эксплуатационных кадров, официальные стажировки и сертификацию (национальную и международную) специалистов по безопасности в зависимости от потребностей отрасли и государства. Стратегия также должна предусматривать специальную подготовку государственных служащих, занимающихся вопросами внутренней и внешней политики, включая сотрудников регуляторных и законодательных органов. Обучение следует

дополнить инициативами по управлению киберрисками, а также практическими занятиями, такими как учения и моделирование, в рамках государственных структур и между ними, а также в организациях других заинтересованных сторон.

Стратегия также должна содействовать инициативам, направленным на развитие специализированных путей карьерного роста в области кибербезопасности и обеспечение эффективного набора будущих сотрудников, в частности для государственного сектора, а также находить стимулы для увеличения предложения квалифицированных специалистов в области кибербезопасности и содействия удержанию кадров. Эти инициативы и стимулы следует разрабатывать в партнерстве с научными учреждениями, частным сектором и гражданским обществом. Чтобы устранить сохраняющийся гендерный разрыв среди специалистов по кибербезопасности, следует применять гендерно сбалансированный подход, мотивирующий, поощряющий и способствующий более активному участию женщин во всех программах, направленных на развитие навыков и обучение, что гарантирует инклюзивность в будущем.

5.5.4 Реализация программы повышения осведомленности в области кибербезопасности

Организации, ответственные за кампании и деятельность по повышению осведомленности в области кибербезопасности на общенациональном уровне, должны в сотрудничестве с соответствующими заинтересованными сторонами разрабатывать и реализовывать программы повышения осведомленности в области кибербезопасности, направленные на распространение информации о рисках и угрозах кибербезопасности, а также о передовых методах противодействия им.

Программа повышения осведомленности в области кибербезопасности может включать кампании по повышению осведомленности, ориентированные на широкую общественность, детей или лиц с низким уровнем компьютерной грамотности; образовательные программы, ориентированные на потребителя; а также инициативы по повышению осведомленности, ориентированные на руководителей предприятий государственного и частного секторов и других лиц. Программы повышения осведомленности должны включать соответствующие ключевые показатели эффективности и показатели для измерения их результативности и эффективности.

5.5.5 Содействие инновациям и научно-исследовательским и опытно-конструкторским работам в области кибербезопасности

Стратегия должна способствовать созданию условий, стимулирующих фундаментальные и прикладные исследования в области кибербезопасности в различных секторах и среди разных групп заинтересованных сторон. К таким инициативам относятся, например, обеспечение соответствия исследований целям национальной стратегии кибербезопасности; разработка в государственных научно-исследовательских организациях программ НИОКР, ориентированных на кибербезопасность; эффективная разработка и распространение новых результатов, базовых технологий, методов, процессов и инструментов. Стратегия также должна предусматривать развитие эффективного и достаточно емкого местного рынка услуг кибербезопасности.

Кроме того, в рамках своей стратегии странам следует стремиться к установлению связей с международным научным сообществом в областях знаний, связанных с кибербезопасностью, таких как информатика, электротехника, прикладная математика и криптография, а также в нетехнической сфере – социально-политических науках, исследованиях в области бизнеса и управления, криминологии, психологии и др.

В стратегии следует рассмотреть механизмы стимулирования в виде грантов, закупок, налоговых льгот, конкурсов и других инициатив, поощряющих разработку инновационных решений, продуктов и услуг в области кибербезопасности.

5.5.6 Специальные программы для уязвимых секторов и групп

В стратегии должны быть определены общественные группы, требующие особого внимания, когда речь идет о потенциале кибербезопасности, наращивании потенциала и повышении осведомленности. К ним относятся группы, которые определены как подвергающиеся особому риску или нуждающиеся в расширении прав и возможностей самозащиты, такие как малые и средние предприятия (МСП), организации на базе общин (ОБО), недостаточно обслуживаемые сообщества и/или сообщества с низким уровнем дохода.

Дополнительные источники информации приведены на с. 67.

5.6 Приоритетная область 6. Законодательство и регулирование

В эту приоритетную область входят разработка нормативно-правовой базы для защиты общества от киберпреступности и создание безопасной и надежной киберсреды в соответствии с принципами открытости, соблюдения основных прав человека и доверительной среды (соответственно разделы 4.3, 4.5 и 4.9). Такая база должна предусматривать принятие законодательства, определяющего незаконную кибердеятельность, а также процессуальные инструменты, необходимые для расследования и судебного преследования за эти преступления на национальном уровне и в рамках международного сотрудничества; создание механизмов обеспечения соблюдения; наращивание потенциала для осуществления контроля за исполнением законодательства; институционализацию критически важных объектов; а также международное сотрудничество в борьбе с киберпреступностью. Такая нормативно-правовая база должна учитывать обязательства страны по международному, региональному и национальному законодательству в области прав человека и обеспечивать их соблюдение.

Кибербезопасность, киберпреступность и защита персональных данных – взаимосвязанные понятия. В каждой стране необходимо создать нормативно-правовую базу, которая комплексно и последовательно охватывает эти три области.

Стратегия должна служить основой и руководством при разработке законодательства, чтобы функции и обязанности субъектов, участвующих в обеспечении применения законов, были четко определены, обеспечивая при этом соблюдение существующих правовых принципов и положений. Стратегия должна отображать существующую нормативно-правовую базу, включая операционные аспекты, и определять области, в которых требуется новое или пересмотренное законодательство и регулирование.

5.6.1 Создание внутренней правовой базы по кибербезопасности

Стратегия должна поощрять разработку внутренней правовой базы в области кибербезопасности и защиты данных, относящейся к действиям по предотвращению, контролю и урегулированию инцидентов, связанных с кибербезопасностью, а также к любым другим действиям, которые государственные и частные организации должны предпринимать для обеспечения безопасного и устойчивого национального киберпространства.

В условиях отсутствия в настоящее время международно-правового документа, определяющего аспекты регулирования кибербезопасности, стране придется создать свои собственные правовые основы кибербезопасности, полагаясь на региональную и/или национальную передовую практику. Основываясь на действующих законах и нормативных актах, касающихся таких аспектов, если таковые имеются, стратегия должна создавать, обновлять или реформировать правовую базу кибербезопасности, включающую, помимо прочего, правила информационной безопасности и их применимость к обеспечению безопасности информационных систем; определение национальной критически важной

информационной инфраструктуры; создание общенациональных и отраслевых учреждений, занимающихся аспектами кибербезопасности (национального агентства по кибербезопасности, национальных и отраслевых CERT/CSIRT/CIRT); сертификацию организаций, процессов, продуктов и политики в области кибербезопасности; правила национальной/государственной безопасности, применимые к безопасности киберпространства; и другие соответствующие вопросы.

Кроме того, в стратегии должны содержаться рекомендации по применению общих подходов к регулированию, касающихся как кибербезопасности, так и киберпреступности (межотраслевой обмен информацией и механизмы обмена оперативными данными, отчетность и статистика уголовного правосудия, государственно-частное сотрудничество и совместное реагирование и др.).

5.6.2 Создание внутренней правовой базы по киберпреступности и электронным доказательствам

Стратегия должна способствовать развитию внутренней правовой базы, которая четко определяет, что такое киберпреступность и связанные с ней уголовные преступления, и обеспечивает надлежащие процессуальные полномочия для эффективного расследования и судебного преследования, а также для вынесения решения по соответствующим делам на основе допустимых электронных доказательств.

Чаще всего эта правовая база принимает форму законодательства о киберпреступности, которое формируется путем принятия новых конкретных законов или внесения поправок в существующие (уголовный кодекс; законы, регулирующие банковскую деятельность, электросвязь и другие отрасли). В этих законах должны быть указаны основные уголовные преступления (преступления против компьютерных систем или данных или осуществляемые с их помощью); процессуальные средства сбора электронных доказательств (от сохранения целостности данных до обыска и изъятия, от производственного заказа до перехвата данных в режиме реального времени); а также инструменты для оперативного и эффективного международного сотрудничества в подобных делах. Чтобы создать четкое и применимое международное законодательство о киберпреступности, странам следует попытаться согласовать свою внутреннюю правовую базу с существующими международными и региональными правовыми инструментами по этим вопросам.

Стратегия также должна содержать указания по оперативным аспектам расследования киберпреступлений и судебного преследования (создание специализированных подразделений, надлежащие возможности цифровой криминалистики, стандартные операционные процедуры, отчетность о преступлениях и т. д.), которые могут не быть включены в законодательную базу, но тем не менее могут быть использованы в качестве вторичных правил, руководящих указаний или примеров передовой практики.

Стратегия также должна содействовать созданию механизма для контроля за исполнением и пересмотром законодательства и инструментов управления, выявления пробелов и случаев дублирования полномочий, а также уточнения и определения приоритетности тех областей, в которых требуется модернизация (например, существующих законов, таких как старые законы об электросвязи).

5.6.3 Признание и гарантирование прав и свобод личности

Стратегия должна способствовать развитию внутренних правовых рамок в области кибербезопасности, киберпреступности и в других смежных областях, обеспечивающих уважение и защиту прав человека. При этом необходимо должным образом подчеркнуть и учесть контекстные различия между кибербезопасностью (техническими аспектами безопасности) и киберпреступностью (уголовно-правовыми мерами).

В стратегии следует уделять особое внимание юридическим вопросам, связанным с информационными технологиями, которые могут влиять на уровень кибербезопасности и нарушать права человека (шифрование, раскрытие информации об уязвимостях, угрожающее анонимности, тест на проникновение и т. п.). При этом стратегия должна поощрять подходы, не нарушающие права человека.

Касательно вопросов киберпреступности и уголовного правосудия в целом, стратегия должна защищать основные процессуальные права, применимые к уголовным расследованиям и судебному преследованию, а также права на неприкосновенность частной жизни и защиту персональных данных и свободу выражения мнений в соответствии с принципом основных прав человека и доверительной среды (разделы 4.5 и 4.9).

Стратегия также должна обеспечивать достаточный учет и защиту прав тех, кто стал жертвой киберинцидентов и киберпреступности или подвергается риску в результате таких инцидентов.

5.6.4 Создание механизмов обеспечения соблюдения

Стратегия должна способствовать созданию внутренних механизмов обеспечения соблюдения (как правоприменительных, так и стимулирующих). Эти механизмы предназначены для предотвращения, пресечения и смягчения последствий действий, направленных против конфиденциальности, целостности и доступности систем и инфраструктур ИКТ, а также угроз для компьютерных данных в соответствии с вышеупомянутой правовой базой. Помимо прочего, они должны учитывать особенности реагирования на киберинциденты, охватывать уголовные расследования, специальные процедуры (такие как законный перехват сообщений) и использование электронных доказательств.

5.6.5 Содействие созданию потенциала для охраны правопорядка

Стратегия должна поощрять развитие потенциала правоохранительных органов в области кибербезопасности, включая подготовку и обучение представителей заинтересованных сторон, участвующих в борьбе с киберпреступностью (судей, прокуроров, адвокатов, сотрудников правоохранительных органов, судебно-медицинских экспертов, финансовых следователей и др.). Правоохранительные органы должны пройти специальную подготовку по интерпретации и применению национальных законов о киберпреступности (то есть переводить закон в технические понятия и наоборот); эффективному выявлению, пресечению, расследованию киберпреступления и преследования их виновников в судебном порядке с соблюдением прав человека; а также научиться эффективно сотрудничать с отраслевыми и международными правоохранительными органами (Интерпол, Европол и др.) в целях борьбы с киберпреступностью и повышения уровня кибербезопасности. Такая подготовка и обучение должны производиться непрерывно и охватывать всех соответствующих специалистов в области уголовного правосудия и безопасности, и содержание этих курсов следует постоянно обновлять с учетом текущих проблем и угроз, связанных с кибербезопасностью. Данный элемент должен учитывать приоритетную область 5 "Возможности и создание потенциала, а также повышение осведомленности" (раздел 5.5).

5.6.6 Разработка межорганизационных процессов

Стратегия должна определять и признавать мандаты национальных ведомств, наделенных первичными полномочиями по обеспечению соблюдения законодательства о киберпреступности (в первую очередь органов уголовного правосудия и судебно-медицинских служб), тех, кто несет ответственность за предотвращение киберинцидентов общенационального уровня и реагирование на них (включая защиту критически важной информационной инфраструктуры), а также тех, кто отвечает за обеспечение соблюдения всех международных требований по борьбе с киберпреступностью (например, за обеспечение

соответствия национальных законов обязательствам по международным договорам) и требований разных юрисдикций (например, за международное сотрудничество) (см. также разделы 5.1.3, 5.1.4 и 5.6.6).

5.6.7 Поддержка международного сотрудничества для борьбы с киберугрозами и киберпреступностью

Стратегия должна демонстрировать приверженность делу защиты общества от киберпреступности на мировом уровне путем ратификации, когда это возможно и соответствует общей национальной повестке дня, международных соглашений о киберпреступности или эквивалентных соглашений по борьбе с киберпреступностью, а также путем поощрения механизмов координации для борьбы с международной киберпреступностью. Это предусматривает приведение национального законодательства в соответствие с обязательствами по международным договорам и двусторонними соглашениями, например путем оказания взаимной правовой помощи, обеспечения возможности проведения международных расследований и трансграничного судебного преследования, рассмотрения электронных доказательств и экстрадиции.

Кроме того, стратегия должна признавать важность создания неформальных механизмов, обеспечивающих доверительное сотрудничество и международный обмен информацией, оперативными данными и услугами технической поддержки между организациями по обеспечению кибербезопасности как в государственном, так и в частном секторе.

В частности, исключительно важную роль в борьбе с киберпреступностью играет международное сотрудничество правоохранительных органов в виде обмена информацией, проведения трансграничных расследований, операций и арестов. Например, Интерпол предоставляет странам безопасную глобальную систему полицейской связи для облегчения запросов между полицейскими управлениями и официальных запросов на взаимную правовую помощь от одного центрального органа к другому. Эти каналы могут помочь в расследовании киберпреступлений и судебном преследовании преступников за пределами страны. Сотрудничество правоохранительных органов также может помочь улучшить взаимодействие между юрисдикциями и обеспечить своевременные и скоординированные совместные действия полиции. Сотрудничеству правоохранительных органов на региональном уровне также придают большое значение и другие организации, такие как AFRIPOL, AMERIPOL, ASEANAPOL, GCCPOL, ECOPOL и Europol.

Эти элементы должны учитывать приоритетную область 7 по международному сотрудничеству (раздел 5.7).

Дополнительные источники информации приведены на с. 68.

5.7 Приоритетная область 7. Международное сотрудничество

Эта приоритетная область сосредоточена на элементах, относящихся к внешним обязательствам страны в области кибербезопасности как на региональном, так и на международном уровнях, которые должна охватывать стратегия. Поскольку цифровизация затрагивает все области международных отношений, такие как права человека, социально-экономическое развитие, торговые переговоры, торговые отношения, контроль над вооружениями, использование новых и прорывных технологий, безопасность цепочек поставок, безопасность, стабильность, мир и разрешение конфликтов, кибербезопасность становится неотъемлемой частью внешней политики страны.

Поэтому стратегия должна признавать трансграничный характер и международное измерение кибербезопасности и подчеркивать необходимость участия в международных дискуссиях и сотрудничество как с национальными, так и с международными заинтересованными сторонами, а также с организациями гражданского общества, промышленностью и неправительственными организациями. Международное взаимодействие с государственными и частными организациями – ключ к налаживанию конструктивного диалога, развитию механизмов доверия и сотрудничества,

нахождению взаимоприемлемых решений и решению общих проблем, а также к формированию глобального понимания важности вопросов кибербезопасности и способности к восстановлению.

Согласно принципу комплексного подхода и установления адаптированных приоритетов (раздел 4.2) региональное и международное сотрудничество необходимо развивать в соответствии с политическим, социальным, культурным и экономическим положением страны. Приоритеты страны в сфере кибербезопасности должны лежать в основе целей ее внешней политики и соответствовать им, и наоборот.

5.7.1 Признание кибербезопасности компонентом внешней политики и согласование внутренних и международных усилий

Стратегия должна выражать приверженность международному сотрудничеству в области кибербезопасности и признавать вопросы кибербезопасности неотъемлемым компонентом внешней политики страны во всех соответствующих областях, включая международную киберстабильность и торговые переговоры.

В стратегии должны быть четко сформулированы приоритетные области правительства и указаны долгосрочные цели международного сотрудничества, а также участвующие в нем заинтересованные стороны (государственные, частные, региональные и международные и т. д.). К таким приоритетным областям могут, например, относиться поддержка деятельности по установлению международных норм кибербезопасности и мер укрепления доверия (СВМ), стремление к наращиванию потенциала кибербезопасности (ССВ), участие в разработке международных стандартов кибербезопасности, а также присоединение к текущим региональным и международным процессам.

Кроме того, стратегия должна обеспечивать согласованность между повестками дня внутренней и внешней политики страны путем приведения ее национальной правовой базы и политики в соответствие с международными обязательствами и согласования национальных подходов к обеспечению кибербезопасности с ее международными усилиями в этой области. Для этого может потребоваться согласование деятельности различных правительственных структур (таких как глава государства и кабинет министров, министерство иностранных дел, министерство ИКТ, министерство промышленности и торговли, министерство юстиции, министерство обороны и т. д.), с тем чтобы политическая позиция, выражаемая за столом переговоров на международной арене одной национальной организацией, была должным образом скоординирована и согласована с другими государственными органами.

5.7.2 Участие в международных дискуссиях и стремление к реализации

В стратегии должны быть определены конкретные международные форумы и механизмы сотрудничества, к которым страна желает присоединиться или с которыми она хочет сотрудничать, чтобы эффективно участвовать в обсуждении вопросов, связанных с кибербезопасностью, на международном уровне. Это могут быть региональные или глобальные организации, органы по стандартизации, межправительственные или многосторонние обсуждения, союзы организаций государственного и/или частного секторов, а также устоявшиеся традиционные механизмы кооперации и сотрудничества, включающие кибер- или цифровой компонент.

В стратегии должно быть указано на приверженность страны применению международного права, в том числе Устава Организации Объединенных Наций и международного права в отношении прав человека. В ней также может быть изложено обязательство страны по присоединению к существующим региональным и международным документам по борьбе с киберпреступностью и другими киберугрозами (Будапештской конвенции Совета Европы о киберпреступности, Конвенции Африканского союза о кибербезопасности, Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий, Директиве ЭКОВАС о борьбе

с киберпреступностью и др.) и их применению. Стратегия должна признавать,что многие международные торговые соглашения также имеют цифровой или киберкомпонент (например, Вассенаарские договоренности регулируют технологии двойного назначения, а Соглашение между Соединенными Штатами, Мексикой и Канадой (USMCA) и Всестороннее региональное экономическое партнерство (RCEP) между странами Азиатско-Тихоокеанского региона регулируют трансграничные потоки данных).

Стратегия должна также поощрять приверженность страны дальнейшему развитию добровольных норм ответственного поведения государства в киберпространстве и мер укрепления доверия (CBM) в киберпространстве. К известным примерам международных усилий и форумов по разработке таких норм и CBM относятся Рабочая группа открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий (OEWG); инициатива Организации по безопасности и сотрудничеству в Европе (ОБСЕ) в области мер укрепления доверия и международных норм, применимых в киберпространстве; работа подгруппы по преступлениям с использованием высоких технологий Группы 7, а также другие региональные инициативы и мероприятия с участием многих заинтересованных сторон ("Парижский призыв", отраслевые инициативы и т. д.). Важно определить приоритетность усилий по международному взаимодействию, выделить достаточные ресурсы (людские и финансовые) и определить надлежащие полномочия, чтобы гарантировать достижение конкретных результатов.

Стратегия также должна выражать приверженность реализации согласованных норм добровольного поведения государств в киберпространстве, подобных тем, какие были предложены Группой правительственных экспертов ООН (ГПЭ) по достижениям в сфере информатизации и электросвязи в контексте международной безопасности в ее отчете 2015 года, а затем доработаны ГПЭ по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности, завершившей свою работу в мае 2021 года.

5.7.3 Содействие официальному и неофициальному сотрудничеству в киберпространстве

В стратегии должны быть указаны рабочие механизмы международного сотрудничества (как в государственном, так и в частном секторе), к которым страна желает присоединиться. Она может пожелать принять участие в официальных и неофициальных международных усилиях по развитию сотрудничества в области разработки политики и законодательства, правоохранительной деятельности (Интерпол, Европол, ВОИС и др.), реагирования на инциденты, обмена информацией и сообщениями об угрозах (FIRST, ISAC и др.) и т. п. Участие в таких инициативах может способствовать более эффективному сотрудничеству и обмену актуальной и практической информацией о потенциальных угрозах и уязвимостях между соответствующими органами власти, а также координации работы механизмов защиты и реагирования.

В качестве важного компонента усилий по международному сотрудничеству также следует рассматривать трансграничный обмен информацией с организациями частного сектора и предприятиями, занимающимися проблемами кибербезопасности (компании-разработчики антивирусов, сообщество по анализу угроз, глобальные операторы социальных сетей и др.).

5.7.4 Содействие наращиванию потенциала для международного сотрудничества

В стране, которая начинает принимать международные обязательства, от правительства может потребоваться развитие дополнительных компетенций и навыков, связанных с вопросами кибербезопасности, а также повышение общего потенциала для решения постоянно расширяющегося круга проблем кибербезопасности, включая обеспечение международной киберстабильности, защиту данных и неприкосновенности частной жизни, торговлю, коммерцию, контроль над вооружениями, использование новых и прорывных технологий, безопасность поставок и другие вопросы, связанные с цифровыми технологиями.

Чтобы эффективно участвовать в международных дискуссиях и сотрудничестве, важно в дополнение к традиционным методам и процессам дипломатии и торговли поощрять развитие и использование компетенций и навыков, ориентированных на вопросы кибербезопасности (включая кибердипломатию и торговые переговоры). Стратегия может также включать разработку конкретных организационных структур и создание специального учреждения или привлечение обученного персонала, основной задачей которого является дипломатическое взаимодействие по вопросам кибербезопасности, касающимся торговли, дипломатии и международного права.

К другим направлениям деятельности по наращиванию потенциала относятся сотрудничество CERT/CSIRT, сотрудничество правоохранительных и судебных органов, применение международного публичного права, добровольные нормы ответственного поведения государства и т. д. Существуют различные международные программы наращивания потенциала для поддержки таких усилий (GLACY+, Глобальный форум по киберкомпетентности (GFCE), Интерпол и др.). Например, усилия по наращиванию потенциала правоохранительных органов помогут местным и национальным правоохранительным органам усовершенствовать свои навыки, знания и технические возможности в целях использования высокотехнологичных инструментов и систем для предотвращения, обнаружения, расследования и судебного преследования международных киберпреступлений. Они также позволят правоохранительным органам следить за тенденциями в области киберпреступности и постоянно меняющейся ситуации с угрозами, чтобы опережать преступность.

Стратегия должна учитывать существующие региональные и международные инициативы в области кибербезопасности и способствовать их гармонизации и согласованию. Это позволит стране использовать имеющуюся передовую практику, а также способствовать согласованию и сближению подходов к обеспечению кибербезопасности.

Стратегия должна поощрять взаимное обучение и обмен знаниями и навыками в области кибербезопасности с международными партнерами. Участие в международных мероприятиях и учениях по кибербезопасности также может способствовать как наращиванию потенциала в области кибербезопасности, так и укреплению доверия и развитию международного сотрудничества.

Дополнительные источники информации приведены на с. 69.

Раздел 6

Справочные материалы

В процессе разработки настоящего Руководства был проведен анализ имеющихся руководств и примеров передовой практики.

Это позволило нам подобрать имеющиеся материалы, которыми страны могут руководствоваться при разработке своей национальной стратегии кибербезопасности. Ниже представлен полный каталог вышеупомянутых материалов с указанием веб-ссылок.

Жизненный цикл национальной стратегии кибербезопас-ности

Инициирование

CCDCOE. "National Cyber Security Strategy Guidelines", section 1.3, 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)" dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

GPD. "Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers", 2020. https://www.gp-digital.org/publication/involving-stakeholders-in-national-cybersecurity-strategies-a-guide-for-policymakers/

Критический обзор и анализ

CCDCOE. "Cybersecurity Strategy & Governance Repository". https://ccdcoe.org/library/strategy-and-governance/

CCDCOE. "National Cyber Security Framework Manual", sections: 3.4, 4, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections: 2.1, 2.2, 3.2.1, 3.3.1 (2013).

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

GCSCC. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition

GFCE. "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle", sections: 1-7, 2021. https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/

ITU. "Global Cybersecurity Index 2020", 2021. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

OAS. "Managing National Cyber Risk", 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNIDIR. "Cyber Policy Portal", 2021. www.cyberpolicyportal.org

Разработка национальной стратегии кибербезопасности

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1. 1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Реализация

ENISA. "National Cyber Security Strategies: An Implementation Guide", 2012.

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

GCSCC. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition

GFCE. "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle", 2021. https://cybilportal.org/tools/catalog-of-project-options-for- the-national-cybersecurity-strategy-ncs-cycle/

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Контроль и оценка

CCDCOE. "Cybersecurity Strategy & Governance Repository". https://ccdcoe.org/library/strategy-and-governance/

CCDCOE. "National Cyber Security Framework Manual", section 2.4, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework- manual/

ENISA. "National Capabilities Assessment Framework", 2020.

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

OAS. "Managing National Cyber Risk", 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Общие принципы

Концепция

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

Microsoft. "Building an Effective National Cybersecurity Agency", 2018.

Microsoft. "Developing a National Cybersecurity Strategy, Sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline", 2013.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Комплексный подход и установление адаптированных приоритетов

CCDCOE. "Cybersecurity Strategy & Governance Repository". https://ccdcoe.org/library/strategy-and-governance/

CCDCOE. "National Cyber Security Framework Manual", sections: 3.4, 4, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework- manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections: 2.1, 2.2, 3.2.1, 3.3.1 (2013).

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

GCSCC. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition

GFCE. "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle", sections: 1-7, 2021. https:// cybilportal.org/tools/catalog-of- project-options-for-the-national-cybersecurity-strategy-ncs-cycle/

OAS. "Managing National Cyber Risk", 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

UNIDIR. "Cyber Policy Portal", 2021. www.cyberpolicyportal.org

Открытость

Социально-экономическое благополучие

GPD. "Involving Stakeholders in National Cybersecurity Strategies: A Guidefor Policymakers", 2020. https://www.gp-digital.org/publication/involving-stakeholders-in-national-cybersecurity-strategies-a-guide-for-policymakers/

GPD. "Toolkit for Inclusive and Value-Based Cybersecurity Policymaking". https://www. gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/

OECD. "Recommendation of the Council on Digital Security of Critical Activities", 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The- Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document", 2015.

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document", 2015.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Основные права человека

Council of Europe. "Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence – Draft as Approved by the Cybercrime Convention Committee", 2021.

Council of Europe. "Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries", sections 1, 2, 6 (2016).

Council of Europe. "Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region", sections 1, 2, 7 (2013).

CTO. "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 (2015).

ENISA. "National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies", sections 3.15, 3.184.9, 4.12 (2016).

Europe, Council. "Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)", 2004.

ITU. "Guidelines for Policy-Makers on Child Online Protection", sections 3.3, 3.4 (2020). https://www.itu-cop-guidelines.com/policymakers

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 3, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

UN. "Sustainable Development Goals, Article 16.3 UNCTAD, Global Cyberlaw Tracker", 2015.

UNHR. "International Covenant on Civil and Political Rights, Article 19", 1976.

WEF. "Cybercrime Prevention Principles for Internet Service Providers", 2020. https://www.weforum.org/reports/cybercrime-prevention-principles-for- internet-service-providers

WEF. "Partnership against Cybercrime", 2020. https://www.weforum.org/reports/partnership-against-cybercrime

WEF. "Recommendations for Public-Private Partnership against Cybercrime", 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf

World Bank. "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies".

Управление рисками и способность к восстановлению

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

CCDCOE. "National Cyber Security Framework Manual", sections: 3.2, 4.2.2, (2012). https://ccdcoe.org/library/publications/national-cyber-security- framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections 3.5 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCI. "Checklist", 2013.

CTO. "Commonwealth Approach for Developing National Cyber Security Strategies", sections 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31 (2015).

ENISA. "CERT Operational Gaps and Overlaps", 2011.

ENISA. "Good Practice Guide for Incident Management", 2011.

ENISA. "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 (2016).

ENISA. "Strategies for Incident Response and Cyber Crisis Cooperation", 2016.

FIRST. "FIRST CSIRT Services Framework Version 2.1", 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

FIRST. "FIRST PSIRT Services Framework Version 1.1", 2020. https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.2; Dimension 5: 5.6, University Oxford, 2021.

ITU. "CIRT Framework", 2021.

ITU. "Cyber Drill Framework", 2021.

Microsoft. "Developing a National Strategy for Cybersecurity, Section: Building Incident Response Capabilities", 2013.

Microsoft. "Information Sharing Framework for Cybersecurity", 2015.

Microsoft. "Risk Management for Cybersecurity: Security Baselines", 2017.

OAS. "Best Practice for Establishing a National CSIRT", p. 35, 2016.

OAS. "Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity", pp.3-4, 2004.

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity", section 2-B, 2015.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 2,4 (2015). https://www.potomacinstitute.org/images/CRIndex2.0.pdf

TNO. "Getting Started with a National CSIRT Guide", 2021. https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/

UNU. "Report: Cyber Resilience in Asia Pacific – A Review of National Cybersecurity Strategies", 2020. https://collections.unu.edu/view/UNU:7760

WEF and Carnegie. "International Strategy to Better Protect the Financial System Against Cyber Threats", 2020. https://carnegieendowment. org/2020/11/18/international-strategy-to-better-protect-financial-system- against-cyber-threats-pub-83105

WEF. "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", 2020. https://www.weforum.org/whitepapers/cyber-resilience-in-the- electricity-ecosystem-securing-the-value-chain

WEF. "Cyber Resilience: Playbook for Public- Private Collaboration", 2018. https://www.weforum.org/reports/cyber-resilience-playbook-for-public- private-collaboration

WEF. "Pathways Towards a Cyber Resilient Aviation Industry", 2021. https://www.weforum.org/reports/pathways-towards-a-cyber-resilient-aviation-industry

Соответствующий набор инструментов политики

CCDCOE. "National Cyber Security Strategy Framework Manual", section 5, 2012. https://ccdcoe.org/library/publications/national-cyber-security- framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", section 3.2, 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCI. "Checklist", 2013.

CTO. "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 (2015).

ENISA. "National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies", sections 3.15, 3.184.9, 4.12 (2016).

Europe, Council. "Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)", 2004.

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)". Dimension 4: 4.1, 4.3, 4.4, University Oxford, 2021.

Четкое руководство, распределение функций и ресурсов

CCDCOE. "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 (2012). https://ccdcoe.org/library/ publications/national-cyber-security-framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections 1.1, 3.3, 3.8 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CTO. "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 (2015).

ENISA. "An Evaluation Framework for National Cyber Security Strategies", sections 2, 2.2.1, 3.1.1, 3.1.2, 3.1.3 (2016).

ENISA. "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 (2016).

ENISA. "National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace", sections 4, 6 (2016).

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, 1.2, University of Oxford (2021). (https://gcscc.ox.ac.uk/cmm-2021-edition)

GPD. "Toolkit for Inclusive and Value-Based Cybersecurity Policymaking". https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/

Microsoft. "Building an Effective National Cybersecurity Agency", 2018.

Microsoft. "Developing a National Cybersecurity Strategy, Sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline", 2013.

Доверительная среда

ENISA. "National Cyber Security Strategies: An Implementation Guide", 2012.

ENISA. "National Cyber Security Strategies: Training Tool", 2016.

GCSCC. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition

GFCE. "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle", 2021. https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Приоритетные области

ПО 1. Управление

CCDCOE. "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 (2012). https://ccdcoe.org/library/ publications/national-cyber-security-framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections 1.1, 3.3, 3.8 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCI. "Checklist", 2013.

CTO. "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 (2015).

ENISA. "An Evaluation Framework for National Cyber Security Strategies", sections 2, 2.2.1, 3.1.1, 3.1.2, 3.1.3 (2016).

ENISA. "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 (2016).

ENISA. "National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace", sections 4, 6 (2016).

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, 1.2, University of Oxford (2021). (https://gcscc.ox.ac.uk/cmm-2021-edition)

GPD. "Toolkit for Inclusive and Value-Based Cybersecurity Policymaking". https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/

Microsoft. "Building an Effective National Cybersecurity Agency", 2018.

Microsoft. "Developing a National Cybersecurity Strategy, Sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline", 2013.

OAS. "Managing National Cyber Risk", 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

OECD. "Recommendation of the Council on Digital Security of Critical Activities", 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The- Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf

OECD. "Cybersecurity Policy Making at a Turning Point, Annex IV", 2012.

OECD. "Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)", 2013.

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document", 2015.

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document", 2015.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

ПО 2. Управление рисками в области национальной кибербезопасности

CCDCOE. "National Cyber Security Framework Manual", sections: 2.1.2, 5.3.2 (2012). https://ccdcoe.org/library/publications/national-cyber-security- framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CTO. "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 (2015).

ENISA. "National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, 2016.

Global Cyber Security Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, 1.2, 1.3; Dimension 2: 2.1; Dimension 3: 3.1, 3.2, 3.4; Dimension 4: 4.1, 4.2, 4.3, 4.4; Dimension 5: 5.1, 5.2, 5.4, 5.5, 5.6, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition

Microsoft. "Developing a National Cybersecurity Strategy. Building a Risk Approach", 2013.

Microsoft. "Risk Management for Cybersecurity: Security Baselines", 2017.

NIST. "Framework for Improving Critical Infrastructure Cybersecurity", 2015.

OAS. "Managing National Cyber Risk", 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

OECD. "Recommendation of the Council on Digital Security of Critical Activities", 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf

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

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 1,2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

UNIDIR. "Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses", 2020. https://unidir.org/publication/supply-chain-security-cyber-age-sector-trends- current-threats-and-multi-stakeholder

WEF. "Principles for Board Governance of Cyber Risk", 2021. https://www.weforum.org/reports/principles-for-board-governance-of- cyber-risk

ПО 3. Подготовленность и способность к восстановлению

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

CCDCOE. "National Cyber Security Framework Manual", sections: 3.2, 4.2.2 (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", section 3.5 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCI. "Checklist", 2013.

CTO. "Commonwealth Approach for Developing National Cyber Security Strategies", sections 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31 (2015).

ENISA. "CERT Operational Gaps and Overlaps", 2011.

ENISA. "Good Practice Guide for Incident Management", 2011.

ENISA. "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 (2016).

ENISA. "Strategies for Incident Response and Cyber Crisis Cooperation", 2016.

FIRST. "FIRST CSIRT Services Framework Version 2.1", 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

FIRST. "FIRST PSIRT Services Framework Version 1.1", 2020. https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.2; Dimension 5: 5.6, University Oxford, 2021.

ITU. "CIRT Framework", 2021.

ITU. "CyberDrill Framework", 2021.

Microsoft. "Developing a National Strategy for Cybersecurity, Section: Building Incident Response Capabilities", 2013.

Microsoft. "Information Sharing Framework for Cybersecurity", 2015.

Microsoft. "Risk Management for Cybersecurity: Security Baselines", 2017.

OAS. "Best Practice for Establishing a National CSIRT", p. 35, 2016.

OAS. "Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity", pp.3-4, 2004.

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity", section 2-B, 2015.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 2, 4 (2015). https://www.potomacinstitute.org/images/CRIndex2.0.pdf

TNO. "Getting Started with a National CSIRT Guide", 2021. https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/

UNU. "Report: Cyber Resilience in Asia Pacific – A Review of National Cybersecurity Strategies", 2020. https://collections.unu.edu/view/UNU:7760

US "National Cyber Incident Scoring System (NCISS) which includes a Cyber Incident Severity Schema (CISS)". https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System

WEF and Carnegie. "International Strategy to Better Protect the Financial System Against Cyber Threats", 2020. https://carnegieendowment. org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105

WEF. "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", 2020. https://www.weforum.org/whitepapers/cyber-resilience-in-the- electricity-ecosystem-securing-the-value-chain

WEF. "Cyber Resilience: Playbook for Public-Private Collaboration", 2018. https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration

WEF. "Pathways Towards a Cyber Resilient Aviation Industry", 2021. https://www.weforum.org/reports/pathways-towards-a-cyber-resilient-aviation-industry

ПО 4. Критически важная инфраструктура и основные услуги

CCDCOE. "National Cyber Security Framework Manual", section 4.5.4, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections 3.4, 3.5, (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CTO. "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 (2015).

ENISA. "An Evaluation Framework for National Cyber Security Strategies", section 4.2, 2016.

ENISA. "Methodologies for the Identification of Critical Information Infrastructure Assets and Services", 2015.

ENISA. "National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies", section 3.6, 2016.

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)". Dimension 1: 1.1, 1.3, University Oxford, 2021.

Meridian and GFCE. "Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers", 2016. https://www.tno.nl/media/10425/companiondocument_gpg_ciip.pdf

Microsoft. "Critical Connections: Protecting Infrastructures, All Sections", 2014.

Microsoft. "Critical Infrastructure Protection: Concepts and Continuum, All Sections", 2014.

Microsoft. "Risk Management for Cybersecurity: Security Baselines", 2017.

OAS. "Report Cybersecurity and Critical Infrastructure in the Americas", 2015.

OECD. "Recommendation of the Council on Digital Security of Critical Activities. https://Ccdcoe.Org/Uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf

Potomac Institute for Policy Studies (2015): Cyber Readiness Index 2.0", 2019. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

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

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 2.4, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

UNIDIR. "International Cooperation to Mitigate Cyber Operations against Critical Infrastructure", 2021. https://unidir.org/criticalinfrastructure

UNOCT, CTED and INTERPOL. "Compendium of Good Practices for the Protection of Critical Infrastructure against Terrorist Attack", 2018. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/_eng_compendium-cip-final-version-120618.pdf

ПО 5. Возможности и создание потенциала, а также повышение осведомленности

"Council of Europe, Capacity Building Programmes", n.d.

CCDCOE. "National Cyber Security Strategy Framework Manual", sections 4,5.5, 4.6.3 (2012).

CCDCOE. "National Cyber Security Strategy Guidelines", 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCI. **"**Checklist**"**, 2013.

CCI. "Commonwealth Network of Contact Persons Framework", 2005.

CCI. "Harare Scheme on Mutual Legal Assistance in Criminal Matters", 2011.

Council of Europe. "Capacity building programmes". https://www.coe.int/en/web/cybercrime/capacity-building-programmes

Council of Europe. "Cybercrime Octopus Community (Country Resources,Training Materials, Guides and Research". https://www.coe.int/en/web/octopus/home?desktop=true

CTO. "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 (2015).

ENISA. "CERT Operational Gaps and Overlaps", p. 6, 16, 19, 21, 27, 29, 31, 32, 50, 57 (2011).

ENISA. "Cybersecurity Skills Development in the EU", 2020.

ENISA. "Good Practice Guide for Incident Management" p.19, 23, 26, 32, 46, 56, 58, 64, 69 (2010).

ENISA. "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 (2016).

ENISA. "Strategies for Incident Response and Cyber Crisis Cooperation,Section", section 2.1 (2016).

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)". Dimension 3: 3.1, 3.2, 3.3, 3.4, University Oxford, 2021.

ITU. "CIRT Framework", 2021.

ITU. "CyberDrill Framework", 2021.

Microsoft. Developing a National Strategy for Cybersecurity, Section: Driving Research and Technology Investment, Public Awareness. Workforce Training and Education, 2013.

NIST. "Workforce Framework for Cybersecurity NICE Framework", 2020. https://doi.org/10.6028/NIST.SP.800-181r1

OAS. "Cyber Security Awareness Campaign Toolkit, All Sections", 2015.

OAS. "Cybersecurity Education: Planning for the Future Through Workforce Development", 2020.

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity", section 2-B, 2015.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 2.5, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

UNCTAD. "Programme on E-Commerce and Law Reform", 2015.

US "National Cyber Incident Scoring System (NCISS) which includes a Cyber Incident Severity Schema (CISS)". https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System

ПО 6. Законодательство и регулирование

CCDCOE. "National Cyber Security Strategy Framework Manual", section5, 2012. https://ccdcoe.org/library/publications/national-cyber-security- framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", section 3.2, 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCI. "Checklist", 2013.

Council of Europe. "Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence – Draft as Approved by the Cybercrime Convention Committee", 2021.

Council of Europe. "Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries", sections 1, 2, 6 (2016).

Council of Europe. "Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region", sections 1, 2, 7 (2013).

CTO. "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 (2015).

ENISA. "National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies", sections 3.15, 3.184.9, 4.12 (2016).

Europe, Council. "Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)", 2004.

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)". Dimension 4: 4.1, 4.3, 4.4, University Oxford, 2021.

ITU. "Guidelines for Policy-Makers on Child Online Protection", sections 3.3, 3.4 (2020). https://www.itu-cop-guidelines.com/policymakers

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 3, 2015. https ://www.potomacinstitute.org/images/CRIndex2.0.pdf

UN. "Sustainable Development Goals, Article 16.3 UNCTAD, Global Cyberlaw Tracker", 2015.

UNHR. "International Covenant on Civil and Political Rights, Article 19", 1976.

WEF. "Cybercrime Prevention Principles for Internet Service Providers", 2020. https://www.weforum.org/reports/cybercrime-prevention-principles-for- internet-service-providers

WEF. "Partnership against Cybercrime", 2020. https://www.weforum.org/reports/partnership-against-cybercrime

WEF. "Recommendations for Public-Private Partnership against Cybercrime", 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf

World Bank. "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies".

ПО 7. Международное сотрудничество

"Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence – Draft as Approved by the Cybercrime Convention Committee", n.d.

CCDCOE. "National Cyber Security Strategy Framework Manual", sections 4.7, 5.4.2, 5.4.3 (2012). https://ccdcoe.org/library/publications/national-cyber- security-framework-manual/

CCDCOE. "National Cyber Security Strategy Guidelines", sections 1.3, 3.2.1, 3.3.2 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

CCDCOE. "The Tallin Manual 2.0", 2017. https://ccdcoe.org/research/tallinn-manual/

Council of Europe. "Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)", chapter III, 2004.

Council of Europe. "Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries" Strategic Priority 7, 2016.

Council of Europe. "Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region", Strategic Priority 8, 2013.

CTO. "Commonwealth Approach for Developing National Cyber Security Strategies", sections 4.4.20, 4.4.21 (2015).

ENISA. "Guidebook on National Cyber Security Strategies, Section", section 3.16, 2016.

ENISA. "National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies", sections: 3.16. 4.10 (2016).

Global Cyber Security Capacity Center. "Cybersecurity Capacity Maturity Model for Nations (CMM)", Dimension 1: 1.1, 4: 4.4, University Oxford, 2021.

Microsoft. "Developing a National Strategy for Cybersecurity, Section on Structuring International Engagement", 2013.

OECD. "Recommendation of the Council on Digital Security of Critical Activities", 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf

OECD. "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity" p. 13, 48, 58, 2015.

Potomac Institute for Policy Studies. "Cyber Readiness Index 2.0", section 4.6, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

UNIDIR. "Cyber Policy Portal", 2021.

UNIDIR. "International Cooperation to Mitigate Cyber Operations against Critical Infrastructure", 2021. https://unidir.org/criticalinfrastructure

Раздел 7

Акронимы

Акронимы/определения

AFRIPOL	African Union Mechanism for Police Cooperation		Механизм сотрудничества органов полиции Африканского союза
AMERIPOL	The Police Community of the Americas		Полицейское сообщество Северной и Южной Америки
ASEANAPOL	ASEAN Chiefs of Police		Руководители полиции стран АСЕАН
Axon	Axon Partners Group		Группа компаний Axon Partners
CBM	Confidence-building measures		Меры укрепления доверия
CBO	Community-based Organizations		Организации на базе общин
CCB	Commitment to cybersecurity capacity-building		Приверженность наращиванию потенциала в области кибербезопасности
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence		Центр передового опыта по совместной защите от киберугроз при НАТО
CERT	Computer Emergency Response Teams		Группы реагирования на нарушения компьютерной защиты
CII	Critical Information Infrastructures	КИИ	Критически важные информационные инфраструктуры
CIRT	Computer Incident Response Teams		Группы реагирования на компьютерные инциденты
CI	Critical Infrastructures	КИ	Критически важные инфраструктуры
CoE	Council of Europe		Совет Европы
ComSec	Commonwealth Secretariat		Секретариат Британского Содружества
CRI	The Cyber Readiness Institute		Институт киберготовности
CSIRTs	Computer Security Incident Response Teams		Группы реагирования на инциденты компьютерной безопасности
CTO	Commonwealth Telecommunications Organisation		Организация по электросвязи Содружества
DCAF	Geneva Centre for Security Sector Governance		Женевский центр управления сектором безопасности
DNS	Domain Name Service		Служба доменных имен
ECOPOL	ECO Police		Полиция ОЭС
ECOWAS	Economic Community of West African States		Экономическое сообщество западноафриканских государств
Europol	European Police Office		Европейское полицейское управление
FIRST	Forum of Incident Response and Security Teams		Форум групп реагирования на инциденты и обеспечения безопасности
GCCPOL	Gulf Cooperation Council Police		Полиция Совета сотрудничества стран Залива
GCSCC	Global Cyber Security Capacity Centre		Глобальный центр развития потенциала в области кибербезопасности
GCSP	Geneva Centre for Security Policy		Женевский центр политики безопасности
GFCE	The Global Forum on Cyber Expertise		Глобальный форум по киберкомпетентности
GGE	UN Group of Governmental Experts	ГПЭ	Группа правительственных экспертов ООН
GLACY+	Global Action on Cybercrime Extended		Расширенное общество глобальных мер по борьбе с киберпреступностью
GPD	Global Partners Digital		Компания Global Partners Digital
ICT	Information & Communication Technology	ИКТ	Информационно-коммуникационные технологии

INTERPOL	International Criminal Police Organization	Интерпол	Международная организация уголовной полиции
ISAC	Information Sharing and Analysis Centers		Центры анализа и обмена информацией
ITU	International Telecommunication Union	МСЭ	Международный союз электросвязи
IXP	Internet Exchange Points		Пункты обмена интернет-трафиком
KPI	Key Performance Indicators	КПЭ	Ключевые показатели эффективности
NCS	National Cybersecurity Strategy		Национальная стратегия кибербезопасности
OAS	The Organization of American States	ОАГ	Организация американских государств
OEWG	UN Open-ended Working Group		Рабочая группа ООН открытого состава
OSCE	Organisation of Security and Cooperation in Europe	ОБСЕ	Организация безопасности и сотрудничества в Европе
PIPS	Potomac Institute for Policy Studies		Потомакский институт политических исследований
R&D	Research and Development	НИОКР	Научно-исследовательские и опытно-конструкторские работы
RCEP	Regional Comprehensive Economic Partnership		Всестороннее региональное экономическое партнерство
SME	Small and Medium Enterprises	МСП	Малые и средние предприятия
UNIDIR	United Nations Institute for Disarmament Research		Институт Организации Объединенных Наций по исследованиям проблем разоружения
UNOCT	United Nations Office of Counter-Terrorism		Контртеррористическое управление Организации Объединенных Наций
UNU	United Nations University		Университет Организации Объединенных Наций
USMCA	United States-Mexico-Canada Agreement		Соглашение между Соединенными Штатами, Мексикой и Канадой
WEF	The World Economic Forum	ВЭФ	Всемирный экономический форум
WIPO	World Intellectual Property Organization	ВОИС	Всемирная организация интеллектуальной собственности