Практические средства обеспечения кибербезопасности

Исследовательский период 2022–2025 годов

Вопрос 3/2

Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

Промежуточный итоговый документ 2023 года

Резюме

На Всемирной конференции по развитию электросвязи, состоявшейся в Кигали в 2022 году, рассматривался мандат исследуемого Вопроса 3/2, в котором основное внимание уделяется обмену опытом по средствам обеспечения кибербезопасности. Угрозы кибербезопасности являются серьезной проблемой во всем мире, поскольку растущая зависимость от технологий приводит к эскалации рисков и последствий кибератак. Средства обеспечения кибербезопасности стали критически важным элементом защиты сетей, систем и данных от злонамеренных действий.

В настоящем отчете представлены вклады и обсуждения по итогам собраний по Вопросу 3/2 и специального семинара-практикума по средствам обеспечения кибербезопасности. Шесть ключевых выводов из этих обсуждений представлены ниже.

1 Различные уровни критичности и риска требуют разных уровней обеспечения безопасности. Оценка рисков помогает определить, какой требуется уровень обеспечения безопасности, с учетом конфиденциальности защищаемых данных и активов, последствий взлома, а также среды угроз.

2 Взаимодействие с партнерскими организациями, отраслью и различными заинтересованными сторонами может быть эффективным способом обеспечения кибербезопасности. Сотрудничество между директивными органами, организациями гражданского общества и отраслью может повысить спрос на безопасность и предоставить необходимую информацию для разработки политики и нормативных актов.

3 Необходимо принимать во внимание развитие регуляторного подхода, основанного на диалоге и консультациях. Средства обеспечения кибербезопасности можно внедрять на добровольной основе, прежде чем они станут обязательными, в зависимости от необходимости принятия более решительных мер по защите от кибератак.

4 Учитывая динамичный ландшафт угроз и эволюцию рисков кибербезопасности, практические средства обеспечения кибербезопасности следует время от времени пересматривать и адаптировать. Регулярные внутренние проверки и данные разведки угроз безопасности считаются передовым опытом.

5 Предпринимаются усилия по информированию потребителей и производителей о важности кибербезопасности и преимуществах выбора более безопасных продуктов. Схемы маркировки кибербезопасности и образовательные кампании помогают информировать пользователей о безопасности технологических продуктов.

6 Соглашения на основе взаимности упрощают соблюдение требований участниками отрасли, работающими на нескольких рынках, а согласование базовых требований безопасности снижает регуляторную нагрузку на поставщиков продуктов и услуг.

Введение

В ходе последней Всемирной конференции по развитию электросвязи, состоявшейся в Кигали, Руанда, в июне 2022 года, мандат исследуемого Вопроса 3/2 "Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности" был пересмотрен, и одной из конкретных проблем, определенных для изучения, было: "обмен опытом по средствам обеспечения кибербезопасности"[1].

Согласно утвержденному кругу ведения по исследуемому Вопросу 3/2, признается, что угрозы кибербезопасности остаются серьезной проблемой для правительств, организаций и отдельных лиц во всем мире. С ростом зависимости от технологий потенциальные риски и последствия кибератак также возрастают, а кибератаки становятся все более прибыльными[2]. Киберпреступники ведут прибыльный бизнес, который оценивается в 8 триллионов долларов США по всему миру[3].

Средства обеспечения кибербезопасности[4] стали критически важным элементом защиты сетей, систем и данных от злонамеренных действий. В широком смысле к ним относятся процедуры, используемые для обеспечения наличия соответствующих средств контроля для защиты конфиденциальности, целостности и доступности электронных устройств, систем, сетей и данных. Хотя они напрямую не предотвращают кибератаки, их цель, если она правильно реализована, состоит в том, чтобы свести к минимуму риск таких атак. Средства обеспечения кибербезопасности можно проверять на соответствие конкретным мерам контроля безопасности, руководящим принципам и стандартам, при этом они могут либо вводиться нормативными актами, либо на добровольной основе приниматься отраслью. Однако не существует универсального подхода, поскольку национальные органы власти и отраслевые регулирующие органы часто используют разные средства – от самооценок и добровольных руководящих принципов до схем маркировки и жестких проверок соответствия.

При всей невозможности рекомендовать некий единый подход в последние годы и месяцы во всем мире, очевидно, наблюдается устойчивый переход к принятию средств обеспечения кибербезопасности с различными изменениями в нескольких странах и регионах. В качестве примера этого движения следует отметить, что Организация экономического сотрудничества и развития в декабре 2022 года выпустила Рекомендацию Совета по цифровой безопасности продуктов и услуг, в которой рекомендуется принятие правил повышения цифровой безопасности продуктов и услуг пропорционально риску, начиная с подхода, основанного на добровольных политических мерах, и изучение необходимости обязательных мер[5].

В настоящем отчете представлены вклады и обсуждения по итогам собраний по исследуемому Вопросу 3/2 и специального семинара-практикума по средствам обеспечения кибербезопасности. Открытый семинар-практикум, прошедший в Женеве в течение дня 23 мая, стал возможностью изучить глобальный ландшафт обеспечения кибербезопасности в различных областях (интернет вещей (IoT), электросвязь и т. д.), продемонстрировав множество текущих практических средств и идей со всего мира. В нем приняли участие представители Государств-Членов, отрасли, технических органов и гражданского общества.

Руководство Группы Докладчика по исследуемому Вопросу 3/2 хотело бы воспользоваться этой возможностью, чтобы поблагодарить всех докладчиков и участников за их ценный вклад в обсуждение данной темы. Эти усилия были бы невозможными без их целенаправленной работы.

В свете полученных ценных вкладов, в настоящем отчете речь, преимущественно, идет об актуальных проблемах, оценке воздействия и извлеченных на сегодняшний день уроках в процессе рассмотрения и внедрения средств обеспечения кибербезопасности с разделением презентации на шесть выводов.

Эти выводы могут дать членам МСЭ полезную основу для оценки существующих средств и анализа необходимости принятия дополнительных или отличных подходов с учетом опыта и уроков, извлеченных другими администрациями и организациями.

Вывод 1: Различные уровни критичности и рисков требуют разных уровней обеспечения безопасности

При рассмотрении вопроса о внедрении средств обеспечения кибербезопасности важно сначала определить, что пытается защитить организация и какие риски связаны с определенными активами. Страны и компании, желающие защитить себя от кибератак, должны в приоритетном порядке определить, какие системы и активы нуждаются в защите, и оценить их уязвимости. В связи с этим полезным инструментом является наличие плана проведения оценки рисков. Одним из наиболее известных подходов является структура кибербезопасности Национального института стандартов и технологий (NIST)[6], которая обновляется в настоящее время[7] и предлагает широко используемый подход для содействия определению и минимизации организационных рисков. На ее основании устанавливают нерегуляторные руководящие принципы, позволяющие организациям во всем мире определять собственный ландшафт рисков и применять соответствующие меры контроля кибербезопасности в связи с ним. Пересмотренная структура, работа над которой должна быть завершена в начале 2024 года, основывается на широком и долгосрочном взаимодействии с сообществом заинтересованных сторон, которые пользуются этими руководящими принципами, а также на постоянном согласовании с другими международными стандартами.

---

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/ToR/Q3-2.aspx#Question

2 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090023PDFE

3 https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023

4 Оперативная безопасность неразрывно связана со средствами обеспечения кибербезопасности, поскольку она может составлять хорошую основу для них. Broadcom, заместитель председателя ИК 17 МСЭ-Т, представил модель хороших условий, отметив, что она состоит из четырех ключевых элементов: люди и процессы, знания, продукты безопасности (экзогенная безопасность) и безопасность в активах (эндогенная безопасность). См. "Снижение риска и защита репутации", https://www.itu.int/md/T22-SG17-C-0214/en

5 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

6 https://www.nist.gov/cyberframework

7 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

На семинаре-практикуме представитель NIST подчеркнул тот факт, что выгодное положение организации как нерегуляторного органа позволило глубже взаимодействовать с заинтересованными сторонами отрасли по всему миру, чтобы понять реальные проблемы и получить комментарии, которая были учтены в новых руководящих принципах[8]. Эти принципы должны быть адаптируемыми и гибкими с возможностью применения ко всем организациям и секторам. Представитель BitSight, Члена Сектора МСЭ-D, представляющего частный сектор, рассказал о своей платформе, которая включает структуру кибербезопасности NIST и используется различными правительственными учреждениями, отвечающими за кибербезопасность (такими как группы реагирования на нарушение компьютерной защиты (CERT), национальные агентства кибербезопасности, регуляторные органы электросвязи)[9]. Посредством этой платформы страны могут проводить оценку рисков инфраструктуры и активов, считающихся критически важными, и измерять свои факторы риска.

Оценка рисков также помогает определить, какой уровень обеспечения безопасности является приемлемым с учетом конфиденциальности защищаемых данных и активов, последствий, которые будет иметь нарушение, а также среды угроз (например, восприимчива ли организация к кибератакам). В некоторых случаях уровни обеспечения безопасности диктуются нормативными требованиями. Чем выше уровень, тем строже меры безопасности. Например, при низком уровне обеспечения безопасности может быть достаточно системного пароля или брандмауэра, тогда как при более высоком уровне необходимо добавить более развернутые элементы управления, такие как расширенное шифрование и многофакторная аутентификация.

Хотя средства обеспечения кибербезопасности требуют увеличения бюджетов информационных технологий, неспособность внедрить их может оказаться еще более дорогостоящей. В ходе семинара-практикума представители призвали присутствующих задуматься не только о финансовых затратах, связанных с кибератакой, но и о дополнительных репутационных издержках, которые могут быть гораздо более разрушительными. Потеря доверия клиентов и граждан связана с долгосрочными последствиями, не ограничивающимися денежным выражением, и организации должны быть в состоянии стратегически понять это. В равной степени, в государственном секторе успешные атаки могут влиять на предоставление государственных услуг и критически важную деятельность, нарушение которой также невозможно оценить только с финансовой точки зрения, поскольку это влияет на жизнь граждан.

Вывод 2: Взаимодействие с партнерскими организациями, отраслью и различными заинтересованными сторонами может быть эффективным способом обеспечения кибербезопасности

Во-первых, важно сравнивать одни инициативы с другими, анализировать примеры передового опыта и учиться на чужих успехах и ошибках при разработке собственных инициатив. Во-вторых, важно взаимодействовать с множеством заинтересованных сторон, включая представителей отрасли, чтобы получить важную информацию непосредственно по инициативе в плане развития.

Хотя средства обеспечения кибербезопасности становятся все более необходимыми в менее развитых странах, они все еще могут быть труднореализуемыми. Представитель организации Cyber Defense Africa (CDA) в Того объяснил проблемы, с которыми сталкивается местный рынок в плане обеспечения кибербезопасности операторами базовых услуг (ESO)[10]. Среди факторов, которые необходимо рассматривать, были названы такие темы, как недостаток финансирования, недостаток доверия к правительству как поставщику услуг и недостаток местного человеческого потенциала и возможностей. В целях поддержки ESO при соблюдении недавно опубликованных мер контроля кибербезопасности правительство Того создало государственно-частное партнерство с крупным авторитетным поставщиком услуг кибербезопасности для работы в государственном и частном секторах. В рамках этой модели в Того была создана CDA как самодостаточный и высококачественный местный поставщик услуг кибербезопасности, поддерживающий ESO на необязательной основе. Используемая самодостаточная модель позволила Того принять меры в отношении многих проблем, упомянутых выше, приступить к подготовке местных специалистов в области кибербезопасности и стимулировать развитие местного рынка. Представитель отметил важность CDA как частного лица на конкурентном рынке для обеспечения адаптивности, высокого качества услуг и конкурентного ценообразования.

Также важно укреплять сотрудничество между директивными органами, которые могут установить регуляторную среду, и организациями гражданского общества, которые могут повысить спрос на безопасность, а также предоставить информацию для разработки политики и регуляторных основ, опираясь на существующие и накопленные региональные и международные практические подходы. Например, DiploFoundation является международной организацией, предоставляющей учебные программы и средства наращивания потенциала правительствам, регуляторным органам, бизнесу и гражданскому обществу по актуальным вопросам, связанным с кибербезопасностью. Данная организация является участником Женевского диалога по ответственному поведению в киберпространстве (Женевского диалога)[11]. В 2020 году результатом Женевского диалога стал сборник примеров передового опыта[12], в который вошли предлагаемые определения безопасного проектирования и управления уязвимостями, моделирования угроз, безопасности третьих сторон и цепочки поставок, безопасной разработки, управления уязвимостями и раскрытия информации, а также положений организационной культуры. Глобальный форум по кибер-экспертизе (GFCE) является международной платформой, поддерживающей координацию проектов, содействие обмену знаниями и опытом, сопоставление запросов с предложениями о поддержке наращивания потенциала и разработке исследовательских проектов[13]. В рамках GFCE создано четыре региональных центра – в островных государствах Тихого океана, в Африке, в Северной и Южной Америке и Карибском бассейне, а также в Юго-Восточной Азии. Учитывая его глобальное присутствие и разного рода поддержку

[8] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090017PDFE
[9] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090024PDFE
[10] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090025PDFE
[11] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090020PDFE
[12] https://genevadialogue.ch/goodpractices/
[13] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090021PDFE

в развивающихся странах, Форум является отличной площадкой для обнародования еще большего количества различных региональных взглядов на потребности и спрос на наращивание киберпотенциала. GFCE имеет онлайн-портал, который служит хранилищем осуществленных и текущих проектов в области наращивания киберпотенциала во всем мире, а также ресурсов и инструментов. Такой портал также способствует сокращению дублирования усилий и помогает выявить некоторые программы или пробелы и закономерности в предоставлении услуг по наращиванию потенциала.

Вывод 3: Необходимо принимать во внимание развитие регуляторного подхода, основанного на диалоге и консультациях

Во многих случаях средства обеспечения кибербезопасности будут внедряться на добровольной основе, прежде чем стать обязательными. Переход обычно происходит, когда правительства считают, что отрасль не делает достаточно для обеспечения безопасности продуктов и что потребители не обладают достаточными знаниями, чтобы оценить, являются ли продукты безопасными. Это может привести к тому, что правительства и национальные органы власти начинают действовать и указывают, какими средствами обеспечения безопасности должна пользоваться отрасль. Например, в Бразилии регуляторный орган электросвязи Anatel создал систему органов сертификации и испытательных лабораторий внутри страны для сертификации оборудования, размещаемого в помещениях клиентов (CPE или домашних шлюзов). Подход Anatel традиционно заключался в предоставлении рекомендаций по добровольному обеспечению кибербезопасности в секторе электросвязи. Вместе с тем оценка рисков для поставщиков услуг связи (CPE) показала, что в данном случае, учитывая уязвимости и угрозы, связанные с этим типом оборудования, рекомендаций недостаточно и что необходимо установить обязательные минимальные требования безопасности для таких продуктов. Такие обязательные требования для операторов услуг были опубликованы в начале 2023 года и сосредоточены на таких уязвимостях, как небезопасные пароли и ненужные компоненты услуг. Требования вступят в силу в начале 2024 года в рамках обязательных лабораторных испытаний для утверждения продукта[14]. По объяснениям Anatel, переход от необязательных рекомендаций к требованию обязательной сертификации кибербезопасности для определенного набора оборудования возможен только после всестороннего обсуждения с сектором.

Аналогичным образом, Национальное агентство по кибербезопасности (NCA) Королевства Саудовская Аравия представило инициативу по созданию независимой экосистемы верификации и валидации (IV&V)[15], предназначенной для тестирования и сертификации продуктов в этой стране с точки зрения обеспечения кибербезопасности на национальном уровне. Кроме того, эта инициатива направлена на определение и классификацию аппаратного и программного обеспечения, являющегося чрезвычайно чувствительным к рискам и угрозам кибербезопасности. Наряду с этим она призвана внести вклад в развитие человеческого потенциала IV&V. При развертывании инициативы дорожная карта учитывает необходимость начать с добровольной программы, прежде чем сделать ее обязательной. Агентство отмечает также важность обеспечения в перспективе "самодостаточности" такой экосистемы, и это направило NCA на стимулирование заинтересованных сторон рынка к проведению такой оценки.

В области безопасности IoT Соединенное Королевство также предоставило тематическое исследование эволюции от добровольного к обязательному подходу. В последние годы Соединенное Королевство решило законодательно закрепить базовые требования безопасности для потребительских продуктов IoT на основе стандарта Европейского института стандартизации электросвязи (ETCИ) EN 303 645 – первого глобально применимого стандарта кибербезопасности для потребительских устройств IoT. В Соединенном Королевстве производители, импортеры и дистрибьюторы должны будут соблюдать три из 13 руководящих принципов безопасности ETSI, и закон дает правительству полномочия принимать дополнительные требования в случае необходимости в зависимости от регулярных оценок угроз. Решение о введении базового уровня требований безопасности последовало за периодом добровольного принятия. В 2018 году страна сформулировала добровольный свод правил[16] по безопасности IoT для потребителей, но соблюдение отраслевых требований оказалось не таким, как ожидалось. Свидетельства, собранные в ходе консультаций, показали, что потребители ценят безопасность и готовы дополнительно платить за безопасные продукты. Тем не менее, угрозы безопасности не подлежат регулированию того же уровня надежности, что и безопасность продукта, что приводит к отсутствию прозрачности со стороны производителей и более медленному принятию правил безопасности. Свидетельства также показали, что рынок потребительских соединяемых продуктов не стимулирует принятие основных функций безопасности, поскольку потребители в подавляющем большинстве считают, что продукты уже безопасны. Режим направлен на устранение этого пробела путем введения обязательных элементов свода правил для того, чтобы производители знали об уязвимостях и предпринимали шаги для их смягчения. Режим PSTI (безопасность продуктов и инфраструктура электросвязи) вступит в силу в апреле 2024 года и будет применяться ко всем потребительским продуктам, которые могут подключаться к интернету[17].

Одной из выявленных проблем является возможное воздействие на малые и микропредприятия, которые могут столкнуться с трудностями в соблюдении нового режима. Правоохранительный орган Соединенного Королевства разрабатывает руководство по смягчению любого рода непропорционального воздействия. В дополнение к работе с отраслью, Соединенное Королевство поделилось информацией о том, что были выявлены три основных требования, которые должны быть обязательными в схеме, и в течение нескольких лет проводилась четкая разъяснительная кампания по ним. За эти годы Соединенное Королевство проводило занятия по процессу внедрения режима, включая требования к паролям, фундаментальную архитектуру продукта, уязвимости и требования к прозрачности безопасности. Оценка воздействия показала, что общие преимущества в связи с сокращением объема кибератак на потребителей и предприятия могут превысить

[14] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090018PDFE
[15] https://nca.gov.sa/en/news?item=535
[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[17] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090014PDFE

затраты, связанные с режимом. Поскольку Закон PSTI 2022 года является первым законодательным актом об обязательном обеспечении кибербезопасности продуктов в мире, затраты на обеспечение соблюдения режима неясны, но первоначальные оценки показывают, что выделенного финансирования будет достаточно.

В некоторых случаях различие между обязательным и добровольным характером средств обеспечения безопасности зависит от того, кем является пользователь или клиент. Например, Республика Корея запустила Программу обеспечения безопасности облачных вычислений (CSAP), в рамках которой проводится сертификация безопасности услуг облачных вычислений[18]. В целом сертификация CSAP является добровольной. Однако клиенты в государственном секторе (т. е. государственные учреждения) обязаны пользоваться облачными услугами, прошедшими сертификацию CSAP в соответствии с установленными правилами, и поэтому поставщики облачных услуг, предоставляющие их государственным учреждениям, должны получить необходимые сертификаты.

Вывод 4: Учитывая динамичный ландшафт угроз и эволюцию рисков кибербезопасности, средства обеспечения кибербезопасности необходимо пересматривать и адаптировать со временем

Проведение регулярных внутренних проверок, которые помогают выявить пробелы в контроле и риск воздействия, а также подписка на данные разведки угроз безопасности считаются передовым опытом. Даже если продукт сертифицирован, в нем могут обнаружиться недостатки безопасности на протяжении его жизненного цикла. Процесс сертификации требует предоставления информации в определенный момент времени и не учитывает динамические изменения угроз в будущем. Недавнее исследование BitSight показало тесную корреляцию между недостаточной "частотой исправлений" уязвимостей и вероятностью возникновения инцидента кибербезопасности[19], указывая на критическое значение обновлений систем сразу же после появления исправлений безопасности с учетом отмечаемых различий в их распределении по всему миру.

Тестирование на проникновение – это проверка средств обеспечения безопасности, позволяющая оценить безопасность ИТ-системы и выявить уязвимости, которые в противном случае могли бы использоваться для ее взлома. Ofcom, регуляторный орган Соединенного Королевства в области связи, добровольно осуществляет схему TBEST с поставщиками услуг электросвязи. Эта схема тестирования на проникновение направлена на стимулирование кибератаки с целью выявления уязвимостей безопасности, которые затем можно устранить посредством принятия корректирующих мер для улучшения состояния сетевой безопасности операторов[20]. Регуляторный орган представил обзор процесса и различных задействованных заинтересованных сторон. В более широком плане данная схема является примером подхода к режиму надзора, реализуемому Ofcom, в рамках которого основное внимание обращается на важность формирования отношений сотрудничества с отраслью, являющейся предметом регулирования. К настоящему времени все поставщики услуг связи Соединенного Королевства на добровольной основе используют схему TBEST или намереваются ее использовать, и по итогам ее применения вносят соответствующие коррективы. TBEST не является "стандартом" или процессом сертификации. Цель состоит в том, чтобы дать поставщикам услуг связи возможность оперативно повышать осведомленность о киберугрозах и внедрять соответствующие изменения с целью улучшения их возможностей в области киберзащиты. Осведомленность о таких уязвимостях и их устранение позволяют оператору гораздо эффективнее организовать защиту своих сетей.

Вывод 5: Предпринимаются усилия по информированию потребителей и производителей о важности кибербезопасности и преимуществах выбора более безопасных продуктов

Были предприняты усилия по информированию общественности о важности кибербезопасности и преимуществах выбора более безопасных продуктов.

Одним из подходов в этом направлении является разработка схемы маркировки кибербезопасности (CLS), которая используется для нанесения маркировки на сертифицированные продукты как это происходит, например, в Сингапуре. Схемы маркировки в первую очередь служат информационным инструментом для потребителей. Агентство кибербезопасности Сингапура (CSA) представило схему маркировки, которая призвана помочь потребителям различать более и менее безопасные устройства IoT[21]. Схема является добровольной (за исключением Wi-Fi маршрутизаторов, для которых она обязательна) и имеет четыре уровня безопасности, при этом уровень 1 является базовым. Уровни 1 и 2 основаны на самооценке производителей, а уровни 3 и 4 включают стороннюю оценку утвержденной лабораторией. Схема является многоуровневой, чтобы стимулировать производителей к включению дополнительных мер безопасности, помимо основных требований. CSA также рассказало о компромиссах, связанных с введением стандартов кибербезопасности, включая риск того, что производители обойдут рынок из-за увеличения затрат на соблюдение. Напротив, цель состоит в том, чтобы изменить мышление производителей, призвав их рассматривать кибербезопасность как фактор, способствующий развитию рынка, а не как издержки. Что касается влияния схемы маркировки кибербезопасности в Сингапуре, то она все еще находится на ранних стадиях процесса, и предпринимаются усилия по поощрению производителей к участию в этой схеме и улучшению их кибербезопасности. В будущем будет снова проведен опрос общественности для оценки осведомленности и поведения потребителей. Затраты на соблюдение для производителей на уровнях 1 и 2 являются минимальными, и существенного увеличения стоимости продукции для потребителей не отмечается. Ожидается, что при наличии добровольной схемы рыночные силы будут способствовать улучшению кибербезопасности среди производителей.

Помимо маркировки, не менее важно инвестировать в технический контроль и повышать осведомленность и просвещенность населения о рисках кибербезопасности, с которыми сталкиваются организации и страны. В настоящее

[18] https://isms.kisa.or.kr/main/csap/intro/index.jsp
[19] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity
[20] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work
[21] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090016PDFE

время наиболее тревожной тенденцией являются атаки программ-вымогателей. Для этих типов атак основным вектором (т. е. способом проникновения преступника в сеть или систему) являются фишинговые электронные письма[22]. В таком контексте киберпреступники часто могут обойти средства контроля безопасности за счет того, что люди просто открывают фишинговые письма. Поэтому для обеспечения кибербезопасности крайне важно уведомлять о таких вопросах граждан и сотрудников предприятий.

Вывод 6: Важно стремиться к заключению международных соглашений о синергии/согласовании и взаимности

Существование соглашений о взаимности между моделями обеспечения кибербезопасности, а именно схемами сертификации и маркировки, может быть определяющим фактором для масштабирования этих средств. Как подчеркнули заинтересованные стороны, соглашения о взаимности упрощают соблюдение требований участниками отрасли, работающими на нескольких рынках. Однако, учитывая, что соглашения о взаимности являются официальным механизмом, который имеет много национальных ограничений и требует времени для утверждения и подписания, имеется потребность в средствах обеспечения кибербезопасности для нахождения синергии с существующими международными подходами, которые соответствуют национальным потребностям и приоритетам. Это позволит снизить регуляторную нагрузку на поставщиков продуктов и услуг с целью исключения противоречивых требований.

CSA подчеркнуло важность международного сотрудничества в разработке и реализации его схемы маркировки кибербезопасности. Сингапур подписал соглашения о взаимном признании с Финляндией и Германией и работает над расширением своих партнерских отношений в этой области. Сингапур рассказал о своем опыте, поделившись информацией о том, что правительства должны действовать на упреждение в плане признания, хотя производители также заинтересованы в поддержке этого процесса, поскольку он снижает бремя повторного тестирования и сертификации, а также открывает доступ к рынку в разных юрисдикциях. Процесс заключается в объединении заинтересованных сторон для согласования требований и установления общих стандартов, которые являются реалистичными и не слишком обременительными.

На европейском уровне Агентство Европейского союза по кибербезопасности (ENISA) имеет мандат на разработку трех схем сертификации, которые будут признаваться на внутреннем рынке, а следовательно, иметь автоматическое "взаимное признание" в Европейском союзе (ЕС). К ним относятся: *схема общих критериев ЕС для продуктов ИКТ*, по которой готовится законодательный акт с целью принятия; *схема облачных услуг,* находящаяся на этапе широкого обсуждения; и, наконец, *схема 5G*, которая находится в разработке[23].

Наряду со взаимностью и учитывая международные рынки, на которых работает отрасль, согласование базовых требований безопасности также является важным фактором. Примером таких усилий являются стандарты ETSI на потребительские товары IoT. Главный вопрос заключается в том, в какой степени будут согласованы различные нормативно-правовые базы и в какой степени они будут связаны посредством одних и тех же международных стандартов. В связи с этим на семинаре-практикуме было отмечено, что усиление и даже поиск подходящего места для диалога является сложной задачей. В сфере согласования деятельность ENISA в области стандартизации кибербезопасности и 5G требует сотрудничества между CEN, CENELEC, ETCИ, ИСО, Ассоциацией GSM МЭК, 3GPP и GlobalPlatform. Одним из основных результатов работы агентства стала консолидация элементов управления безопасностью 5G разных организаций по разработке стандартов (OPC) в одном хранилище[24].

[22] Распространенная тактика, используемая киберпреступниками для того, чтобы обманом заставить людей раскрыть конфиденциальную информацию или загрузить вредоносное ПО, заражающее целевую систему или сеть.

[23] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090019PDFE

[24] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Приложение: Практические средства обеспечения кибербезопасности

Страна или организация	Название видов практики	Тип практики	Сфера охвата практики	Тип подхода	Ссылка
Австралия	Руководящие указания для производителей по обеспечению безопасности IoT на этапе разработки	Руководящие указания	IoT	Добровольный	Ссылка
Австралия	Кодекс практики: обеспечение безопасности интернета вещей для потребителей	Кодекс практики	IoT	Добровольный	Ссылка
Бразилия	Закон 77/2021 – Требования кибербезопасности для оборудования электросвязи	Требования для схемы сертификации	Оборудование электросвязи	Добровольный	Ссылка
Бразилия	Закон 2436/2023 – Минимальные требования кибербезопасности для оценки соответствия оборудования в помещении клиента (CPE)	Требования для схемы сертификации	CPE	Обязательный	Ссылка
Королевство Саудовская Аравия	Независимая экосистема верификации и валидации (IV&V)	Тестирование и сертификация продуктов. Идентификация и классификация устройств и программного обеспечения	Продукты	Первоначально добровольный	Ссылка
Корея (Республика)	Программа обеспечения безопасности облачных вычислений (CSAP)	Схема сертификации	Облако	Комбинированный – добровольный в целом. Обязательный для предоставления облачных услуг государственным учреждениям	Ссылка
Сингапур	Схема маркировки кибербезопасности	Схема сертификации и маркировки	IoT	Комбинированный – в целом добровольный. Обязательный только для домашних маршрутизаторов Wi-Fi	Ссылка
Соединенное Королевство Великобритании и Северной Ирландии	Режим безопасности продуктов и инфраструктуры электросвязи (безопасность продуктов)	Минимальные требования безопасности	Подключаемые продукты	Обязательный	Ссылка
Соединенное Королевство Великобритании и Северной Ирландии	Схема TBEST	Тестирование на проникновение	Сети электросвязи	Добровольный	Ссылка

ITUПубликации

Опубликовано в Швейцарии, Женева, 2022 г.

Правовая оговорка: https://www.itu.int/en/publications/Pages/Disclaimer.aspx

Международный союз электросвязи
Place des Nations, CH-1211 Geneva Switzerland