Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1060

(06/2021)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность информации и сетей – Управление безопасностью

Структура для создания и эксплуатации центра по защите от киберугроз

Рекомендация МСЭ-Т X.1060

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	**X.1050–X.1069**
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ IMT-T	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1060

Структура для создания и эксплуатации центра по защите от киберугроз

Резюме

В Рекомендации МСЭ-Т X.1060 центр по защите от киберугроз (CDC) определен как подразделение, которому отведена центральная роль в обеспечении противодействия рискам кибербезопасности в организации. Структура описана как три процесса – построение, управление и оценка, которые CDC должен реализовать на практике. Описаны также услуги, которые должна предусмотреть организация для принятия более конкретных мер кибербезопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1060	29.06.2021 г.	17-я	11.1002/1000/14721

Ключевые слова

Центр по защите от киберугроз, CIRT, центр обеспечения безопасности (SOC).

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей публикации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения положений настоящей публикации. Однако те, кто будет применять публикацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к базе данных МСЭ-Т по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Риски кибербезопасности оказывают существенное влияние на деятельность организации в целом. Риски, с которыми сталкиваются организации, связаны с изменениями окружающей среды как в социальных, так и в деловых аспектах, а также с внешним воздействием со стороны регуляторных органов и усилением угроз безопасности. Поэтому обязанность высшего руководства (CxO) – управлять в масштабах всей организации мерами по реагированию на эти риски и изменения. Предполагается, что один из важных аспектов реализации мер кибербезопасности – руководство процессами разработки политики безопасности и управления ею в соответствии со стоящими перед организацией задачами – будет осуществлять, а нередко и осуществляет руководитель службы безопасности (CSO) или руководитель службы информационной безопасности (CISO). Для практической реализации мер безопасности необходимо подразделение, которое оказывает поддержку деятельности CSO и CISO, осуществляя стратегическое управление на уровне организации. Такое подразделение названо в настоящей Рекомендации центром по защите от киберугроз (CDC).

В настоящей Рекомендации определена структура для создания CDC, управления им и оценки эффективности его работы. Структура указывает, каким образом CDC должен определять и внедрять услуги безопасности для обеспечения безопасности организации. Описанная здесь структура поможет организации в противодействии рискам кибербезопасности.

Рекомендация МСЭ-Т X.1060

Структура для создания и эксплуатации центра по защите от киберугроз

1 Сфера применения

Настоящая Рекомендация определяет структуру для создания в организации центра по защите от киберугроз (CDC), управления им и оценки эффективности его работы. Структура указывает, каким образом CDC должен определять и внедрять услуги безопасности для обеспечения безопасности организации.

Рекомендация адресована лицам из числа высшего руководства организации, ответственным за безопасность, таким как руководитель службы безопасности (CSO) или руководитель службы информационной безопасности (CISO), а также инспекторы безопасности, которые им помогают.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в другом документе.

3.1.1 аутсорсинг (outsourcing) [b-ITU-T X.1053]: Сценарий, при котором предприятие отдает по контракту один или несколько своих процессов и/или функций сторонней компании. При аутсорсинге предприятие передает свои ресурсы стороннему предприятию, сохраняя способность управлять отношениями с процессами, переданными на аутсорсинг.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин.

3.2.1 Центр по защите от киберугроз (cyber defence centre (CDC)) – подразделение в рамках организации, которое предоставляет услуги по обеспечению безопасности для управления рисками кибербезопасности в своей коммерческой деятельности.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

APT	Advanced Persistent Threat	Устойчивая угроза нового уровня
CDC	Cyber Defence Centre	Центр по защите от киберугроз
CISO	Chief Information Security Officer	Руководитель службы информационной безопасности
CSIRT	Computer Security Incident Response Team	Группа реагирования на инциденты в сфере компьютерной безопасности
CSO	Chief Security Officer	Руководитель службы безопасности

CxO	C-suite		Высшее руководство
IDS	Intrusion Detection System		Система обнаружения вторжений
IPS	Intrusion Prevention System		Система предотвращения вторжений
IT	Information Technology	ИТ	Информационные технологии
SIEM	Security Information and Event Management		Управление информацией о безопасности и администрирование событий
SLA	Service Level Agreement		Соглашение об уровне обслуживания
WAF	Web Application Firewall		Брандмауэр веб-приложений

5 Условные обозначения

Отсутствуют.

6 Структура Рекомендации

Понятие "центр по защите от киберугроз" (CDC) объясняется в разделе 7 настоящей Рекомендации. Раздел 8 содержит обзор структуры для создания и эксплуатации CDC. Более детально эта структура рассматривается в следующих разделах: "Процесс построения CDC" (раздел 9), "Процесс управления CDC" (раздел 10) и "Процесс оценки CDC" (раздел 11). В разделе 12 общее описание услуг по обеспечению безопасности, которые предоставляет CDC, приведено в виде примеров передового опыта, а в Приложении A подробно описана каждая из этих услуг.

7 Общие сведения о центре по защите от киберугроз

Организации принимают меры, направленные на успешное ведение своей предпринимательской деятельности. В целях управления рисками для предпринимательской деятельности руководитель службы информационной безопасности (CISO) формулирует политику безопасности, особенно в части кибербезопасности. Центр по защите от киберугроз (CDC) – это подразделение, реализующее политику безопасности конкретно в виде услуг CDC, которые представляют собой действия по обеспечению безопасности, осуществляемые группами, ответственными за безопасность. В отношении услуг CDC функции безопасности могут определяться как возможности системы по выполнению процессов, связанных с обеспечением безопасности. На рисунке 1 показаны участники процесса и их роли в функционировании CDC.

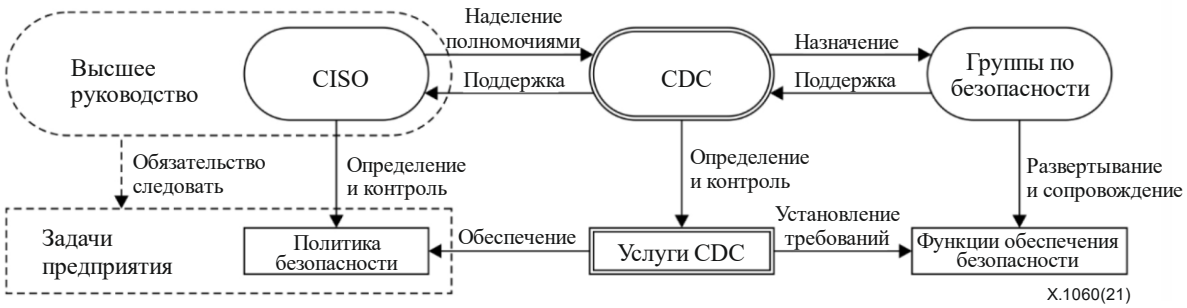

Рисунок 1 – Участники процесса и их роли в эксплуатации CDC

В зависимости от размера и типа организации CDC может представлять собой самостоятельное подразделение, комитет или небольшую группу. В той или иной форме, но CDC должен существовать в организации и ему должны быть предоставлены полномочия и ресурсы для оказания услуг безопасности, позволяющих обеспечить безопасность организации. Такие услуги по обеспечению безопасности должны соответствовать установленной политике безопасности и гарантировать качество мероприятий по обеспечению безопасности. Уровень каждой услуги должен быть четко определен посредством согласованного сторонами документа, например соглашения об уровне обслуживания (SLA). Методика общей оценки качества услуг CDC описана в пункте 9.4.

8 Структура для создания и эксплуатации CDC

На рисунке 2 показана структура для создания и эксплуатации CDC. Она включает три процесса: построение, управление и оценку. Для обеспечения безопасности организации необходимо создать CDC и надлежащим образом управлять им. Кроме того, необходимо регулярно и своевременно оценивать его работу, а также непрерывно ее совершенствовать. Данная структура позволяет организации осуществлять деятельность по обеспечению безопасности.

В процессе построения CDC следует рассмотреть осуществляемые в организации виды деятельности по обеспечению безопасности. В Приложении A приведены примеры передового опыта обеспечения услуг безопасности, предоставляемых CDC. Организация может составить собственный каталог услуг, выбрав услуги из приведенного перечня и дополнив их услугами, отражающими специфику ее работы. Для каждой услуги в каталоге рекомендуется создать профиль, включающий в себя список ответственных за услугу, распределение функций и обязанностей, а также способы исполнения (исполнение собственными силами, аутсорсинг или их сочетание). Установив профили услуг, следует определить текущий и целевой показатели качества каждой услуги CDC для целей оценки.

Процесс управления включает в себя три этапа и два цикла. На этапе стратегического управления осуществляется общее управление деятельностью CDC, на этапе оперативного управления – управление повседневной работой по мониторингу и анализу, а на этапе реагирования – реагирование в чрезвычайных ситуациях. В рамках этих этапов существуют длинный и короткий циклы управления. Оперативное управление и реагирование требуют короткого цикла для своевременного принятия и исполнения решений, а стратегическое управление следует осуществлять по длинному циклу, рассматривая возможность совершенствования в долгосрочной перспективе наряду с результатами, полученными на коротких циклах. Для совершенствования в долгосрочной перспективе, как правило, требуется принимать решения о новых производственных капиталовложениях и коренных изменениях в архитектуре систем.

Процесс оценки предусматривает объективную и своевременную оценку каталога, профиля и портфеля услуг CDC (см. рисунок 4).

Результаты оценки следует учитывать в ходе всех трех процессов, связанных с CDC. Для совершенствования деятельности по обеспечению безопасности в организации должен быть установлен и поддерживаться повторяющийся цикл процессов создания, управления и оценки.

Рисунок 2 – Структура для создания и эксплуатации CDC

9 Процесс построения

9.1 Общие сведения

В процессе построения CDC определяется, какие услуги по обеспечению безопасности следует реализовать в организации. Услуги – кандидаты для реализации выбираются из перечня услуг CDC, который составлен на основе примеров передового опыта в организации. Перечень услуг CDC приведен в разделе 12.

На рисунке 3 показаны три этапа определения набора услуг CDC.

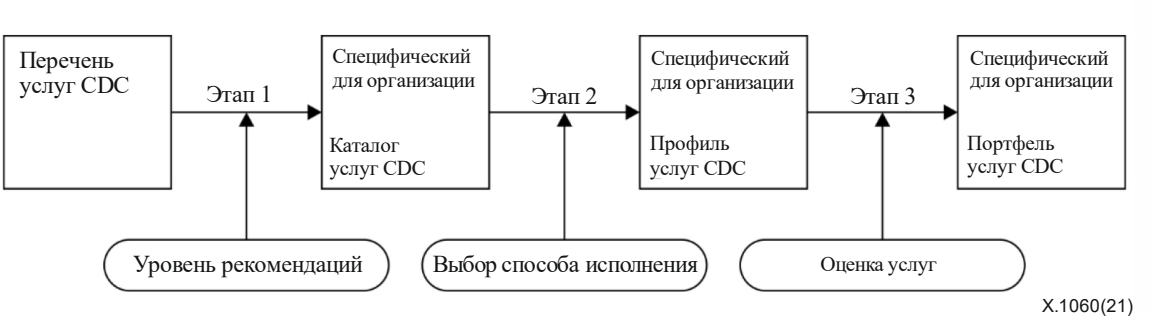

Рисунок 3 – Этапы определения набора услуг CDC

1) Этап 1. Составление каталога услуг CDC

В первую очередь организации следует составить каталог услуг CDC.

На этом этапе из общего перечня услуг отбираются услуги – кандидаты для реализации. Подробная информация об общем перечне услуг приведена в разделе 12. Если необходимые услуги отсутствуют в общем перечне, следует их определить и добавить в каталог услуг CDC.

2) Этап 2. Составление профиля услуг CDC

Для услуг, перечисленных в каталоге услуг CDC, организация должна определить роли и обязанности групп, которые будут предоставлять эти услуги. На этом этапе следует рассмотреть вопрос о способах исполнения услуг CDC согласно рекомендациям из пункта 9.3

По итогам такого рассмотрения организация должна составить профиль услуг CDC.

3) Этап 3. Составление портфеля услуг CDC

Составив профиль услуг CDC, организация должна определить текущий показатель качества (как есть) по каждой услуге и установить средне- или долгосрочный плановый показатель качества (как должно быть).

После определения текущих и плановых показателей качества услуг организация должна составить портфель услуг CDC.

На рисунке 4 показан пример матрицы услуг CDC. Эта матрица будет заполняться в ходе осуществления этапов 1–3.

Услуга	Уровень рекомендаций	Способ исполнения (исполнитель)	Оценка услуги	
			Как есть	Как должно быть
Пример услуги 1	Основные	Собственные силы (отдел АВ)	3	5
Пример услуги2	Стандартные	Аутсорсинг (компания Z-MSSP)	2	4
Пример услуги3	Расширенные	Не может быть предметом передачи	1	2

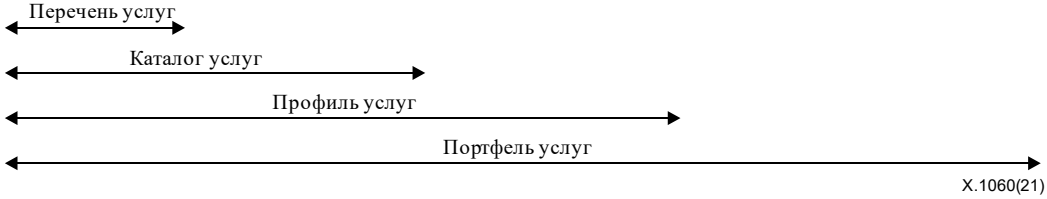

Рисунок 4 – Матрица услуг CDC

9.2 Уровни необходимости услуг CDC

Для того чтобы реализовать услуги CDC в составе, наиболее подходящем для конкретной организации, можно рассмотреть необходимость каждой из них по шкале из пяти уровней, представленной в таблице 1. Определение уровня необходимости позволяет выяснить, насколько приоритетна реализация той или иной услуги.

Таблица 1 – Уровни необходимости услуг CDC

Вес	Описание
Излишние	Услуги, которые не считаются необходимыми
Основные	Минимальный набор услуг, подлежащих реализации
Стандартные	Услуги, широко рекомендованные к реализации
Расширенные	Услуги, требуемые для повышения уровня цикла работы CDC
Необязательные	Услуги, произвольно выбранные в соответствии с предполагаемой формой работы CDC

9.3 Способы исполнения услуг CDC

Организации следует четко определить, какая рабочая группа будет предоставлять ту или иную услугу CDC. В зависимости от возможностей реализации услуг в организации ей следует определить способы исполнения услуг CDC, которые могут включать в себя аутсорсинг (см. таблицу 2).

Таблица 2 – Способы исполнения услуг CDC

Тип	Описание
Исполнение собственными силами	Услуги, предоставляемые группой в рамках организации. Организация должна назначить ответственную группу
Аутсорсинг	Услуги, предоставляемые сторонней группой. Организация должна назначить стороннего подрядчика
Комбинированное исполнение	Организация использует как внутренних, так и сторонних подрядчиков. Организация должна назначить ответственную группу и стороннего подрядчика
Исполнитель не назначен	Услуга признана организацией, но исполнитель ее не назначен

При использовании аутсорсинга следует прояснить пункты A и B.

A) Характер обрабатываемой информации

Организация должна классифицировать обрабатываемую информацию по характеру, в том числе с проведением различий между внутренней или внешней для организации информацией. Например, применительно к инцидентам информация о нанесенном ущербе или последствиях атаки должна считаться внутренней, а информация о самой атаке – внешней.

B) Необходимость в специальных навыках в сфере безопасности

Организации следует рассмотреть вопрос о том, требуются ли специальные навыки в сфере безопасности для предоставления той или иной услуги.

Исходя из этих факторов услуги CDC можно распределить по квадрантам I–IV (см. рисунок 5).

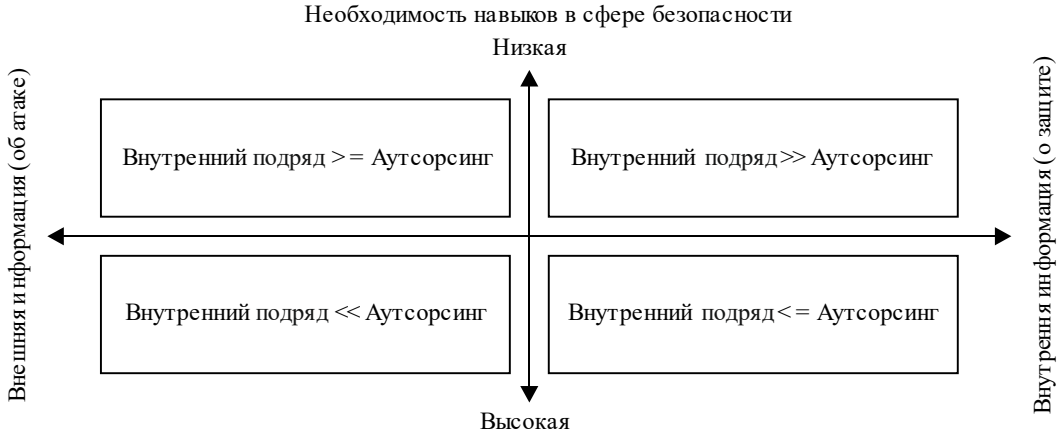

Рисунок 5 – Квадрантная схема привлечения исполнителей

I) Внутренний подряд >> Аутсорсинг

Когда для обработки конфиденциальной информации внутри организации не требуется специальных навыков в сфере безопасности, оптимальным способом является внутренний подряд, и к аутсорсингу лучше не прибегать.

II) Внутренний подряд >= Аутсорсинг

Если требования к квалификации не столь высоки, а информация является внешней для организации, соответствующую деятельность и управление ею следует осуществлять в основном собственными силами организации при поддержке аутсорсинга.

III) Внутренний подряд << Аутсорсинг

Для обработки информации (главным образом об атаках), которая является внешней для организации, услуга должна предоставляться организацией, обладающей специальными навыками (например, сторонним подрядчиком). Если в организации отсутствуют специалисты, обладающие требуемыми навыками, ей будет трудно предоставлять данную услугу самостоятельно.

IV) Внутренний подряд <= Аутсорсинг

Когда для обработки внутренней информации в организации необходимы специальные навыки, осуществление такой деятельности следует в основном поручить специализированной организации (например, стороннему подрядчику), а управление и поддержку этой деятельности оставить за организацией.

9.4 Оценка услуг CDC

Имея подготовленный портфель услуг CDC, следует оценить текущее (как есть) и плановое (как должно быть) состояние реализации каждой услуги по балльной системе, описанной в таблице 3. Следует отметить, что различные типы услуг, например предоставляемых внутренними и сторонними подрядчиками, должны оцениваться по критериям, установленным для балльной оценки.

Таблица 3 – Балльная оценка состояния реализации услуг CDC

Для внутреннего подряда	
Операция задокументирована и разрешена к выполнению CISO или другим директором по организационным вопросам с соответствующим кругом обязанностей	+5 баллов
Операция задокументирована, и роль существующего оператора могут выполнять другие организации	+4 балла
Операция не задокументирована, и роль существующего оператора могут частично выполнять другие организации на временной основе	+3 балла
Операция не задокументирована, и соответствующую роль может выполнять существующий оператор	+2 балла
Операция не выполняется	+1 балл
Решено не выполнять операцию посредством внутреннего подряда	–
Для стороннего подряда	
Содержание услуги и ожидаемый результат понятны, и их результаты соответствуют ожиданиям	+5 баллов
Содержание услуги и ожидаемый результат понятны, но их результаты не соответствуют ожиданиям	+4 балла
Не понятны либо содержание услуги, либо ожидаемый результат	+3 балла
Не понятны ни содержание услуги, ни ожидаемый результат	+2 балла
Не рассматривались ни результаты, ни отчет о них	+1 балл
Решено не выполнять операцию посредством стороннего подряда	–

10 Процесс управления

CDC создает условия для осуществления мероприятий по обеспечению безопасности в масштабах всей организации, реализуя процесс управления, состоящий из трех уровней и двух циклов, как показано на рисунке 6.

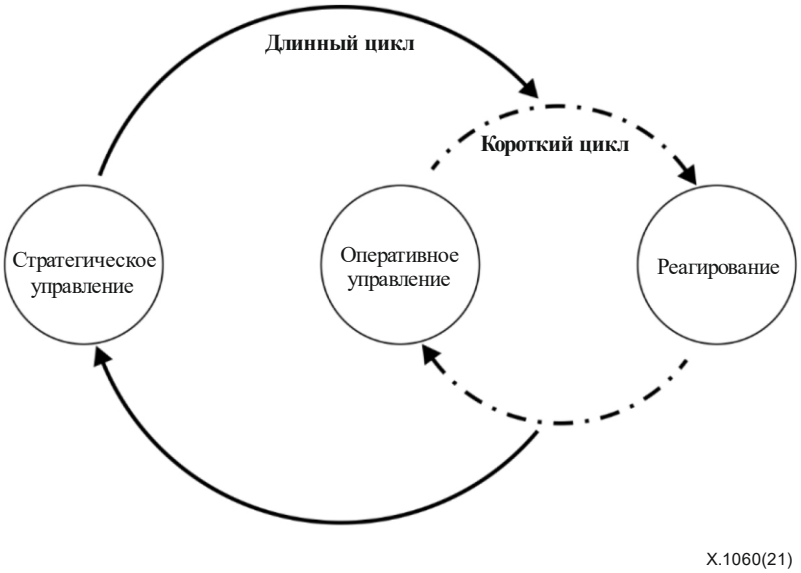

Рисунок 6 – Процесс управления CDC

1) Уровень стратегического управления

Стратегическое управление предполагает ответственность и подотчетность в отношении предоставления всех стратегических услуг, связанных с выработкой определений, проектированием, планированием, управлением, сертификацией и другими видами деятельности, обеспечивающими долгосрочное развитие CDC.

2) Уровень оперативного управления

Техническая поддержка введенной структуры должна осуществляться на уровне оперативного управления. Это повседневная работа, обычно включающая в себя рутинные действия, такие как анализ выявленных инцидентов безопасности, а также мониторинг и обслуживание систем реагирования в сфере безопасности. Группу, выполняющую такие операции, часто называют центром обеспечения безопасности (SOC).

3) Уровень реагирования

Если в ходе анализа на уровне оперативного управления было выявлено представляющее интерес событие, за этим должно последовать реагирование на инцидент. Этот уровень всегда связан с чрезвычайными ситуациями. Группу специалистов, реагирующую на инциденты, часто называют группой реагирования на инциденты в сфере компьютерной безопасности (CSIRT).

Входные данные могут поступать на уровень реагирования не только с уровня оперативного управления, но группа должна также реагировать на отчеты или уведомления от третьих сторон.

A) Короткий цикл

Оперативное управление и реагирование осуществляются ежедневно. На этих уровнях всегда возникают проблемы, связанные с бизнес-процессами и системой реагирования в сфере безопасности. Поэтому в рамках ресурсов (кадры, бюджет, системы), выделяемых в коротком цикле, для решения этих проблем необходимо постоянно вводить усовершенствования, например простую автоматизацию простых задач, улучшение средств анализа точности статей отчета.

B) Длинный цикл

Анализ, требующий выделения новых ресурсов, следует проводить в рамках длинного цикла.

Если анализ короткого цикла выявил проблемы, которые не могут быть решены в рамках текущей системы, следует выработать план на долгосрочную перспективу – например предусматривающий внедрение нового продукта для обеспечения безопасности, коренной пересмотр политики безопасности и крупномасштабное изменение конфигурации систем безопасности.

11 Процесс оценки

11.1 Общие сведения

Каталог, профиль и портфель услуг CDC, созданные в процессе построения, следует регулярно и своевременно оценивать. Процесс оценки услуг CDC показан на рисунке 7.

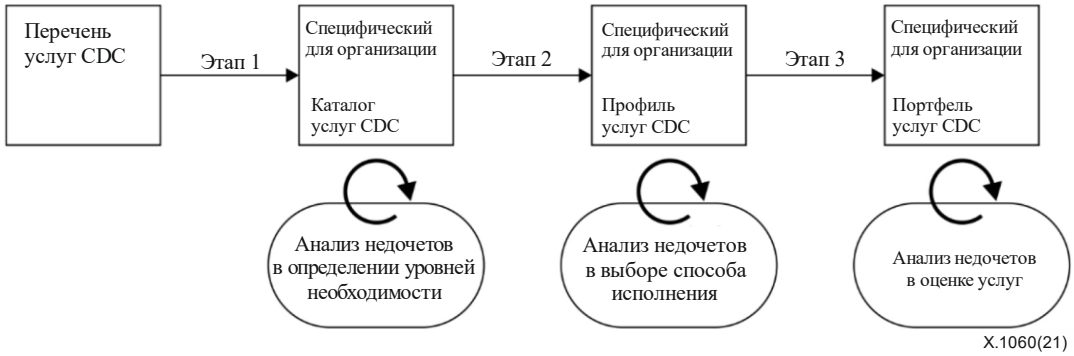

Рисунок 7 – Процесс оценки услуг CDC

11.2 Оценка каталога услуг CDC

Следует выполнить анализ недочетов в определении уровней необходимости услуг CDC. Пересмотр требуется в связи с изменениями обстановки и состава угроз; в частности, следует еще раз изучить и пересмотреть излишние услуги, чтобы убедиться, что ничего не упущено. Оценку каталога услуг CDC следует осуществлять при изменениях в деятельности организации (например, при введении новых видов коммерческой деятельности), а также в ответ на новые риски и угрозы.

11.3 Оценка профиля услуг CDC

Следует выполнить анализ недочетов в выборе способов исполнения услуг CDC. При принятии решения о способах исполнения можно устранить услуги, которые "не могут быть переданы для исполнения", и благодаря такому пересмотру организация может рассчитывать на повышение своего уровня зрелости. Пересматривать профиль услуг CDC следует при возникновении организационных изменений, например при переходе с внутреннего подряда на аутсорсинг и наоборот.

11.4 Оценка портфеля услуг CDC

Следует выполнить анализ недочетов в определении показателей качества отдельных услуг CDC. Следует выяснить причины расхождений между целевыми и текущими показателями качества, чтобы организация могла сосредоточиться на необходимых улучшениях, перепроверить балльные показатели качества услуг CDC и определить недочеты. Оценивать портфель услуг CDC следует на регулярной основе.

12 Категории и перечень услуг CDC

Категории и перечень услуг CDC используются в процессах построения и управления (см. разделы 9 и 10).

Услуги CDC подразделяются на девять категорий:

A) стратегическое управление CDC;

B) анализ в реальном времени;

C) углубленный анализ;

D) реагирование на инциденты;

E) проверка и оценка;

F) сбор, анализ и оценка оперативной информации об угрозах;

G) разработка и обслуживание платформ CDC;

H) поддержка мер реагирования на мошенничество внутри организации;

I) активное взаимодействие с внешними сторонами.

A. Стратегическое управление CDC

К этой категории относятся выработка политики и планирование ресурсов для всех мероприятий по обеспечению безопасности из категорий A–I в организации (включая CDC) в целях обеспечения ее устойчивой работы.

B. Анализ в реальном времени

К этой категории относится непрерывный мониторинг и анализ журналов регистрации и данных из различных систем, таких как сетевые устройства, серверы и продукты для обеспечения безопасности. Цель состоит в обнаружении угроз в реальном времени для оперативного и адекватного реагирования на инциденты.

C. Углубленный анализ

Эта категория связана с расследованием инцидентов – в частности с анализом затронутых систем, данных, конфиденциальность которых нарушена, а также средств и методов, использованных при атаке.

Цель состоит в том, чтобы выяснить весь масштаб инцидента и определить его последствия.

D. Реагирование на инциденты

Эта категория включает в себя конкретные меры противодействия угрозам, основанные на информации об угрозах и результатах анализа в реальном времени.

Цель состоит в том, чтобы минимизировать воздействие на систему и деятельность организации, в том числе на процессы координации действий с заинтересованными сторонами и отчетности перед ними.

E. Проверка и оценка

К этой категории относится оценка уязвимости систем, подлежащих защите, а также обучение реагированию на инциденты и оценка реагирования. Цель этой категории заключается в том, чтобы повысить уровень безопасности.

F. Сбор, анализ и оценка оперативной информации об угрозах

Эта категория включает сбор доступной в интернете информации об угрозах и атаках (внешней оперативной информации), а также обработку информации, касающейся анализа в реальном времени и реагирования на инциденты (внутренней оперативной информации).

Цель – повысить уровень точности анализа в реальном времени и реагирования на инциденты, а также улучшить состояние активов в сфере безопасности.

G. Разработка и техническое обслуживание платформ CDC

К этой категории относится управление имеющимися системами, необходимыми для реагирования на инциденты безопасности, их совершенствование, а также разработка новых таких систем (например, продуктов для обеспечения безопасности, баз данных журналов и операционных систем).

Цель состоит в том, чтобы обеспечить бесперебойное и устойчивое проведение мероприятий по обеспечению безопасности в других категориях.

H. Поддержка мер реагирования на мошенничество внутри организации

В эту категорию входит сбор данных контроля для поддержки мер реагирования на мошенничество внутри организации.

Цель этой категории состоит в том, чтобы оказывать поддержку мерам реагирования на мошенничество внутри организации и его устранения путем предоставления журналов и их анализа.

I. Активное взаимодействие с внешними сторонами

К этой категории относится координация и сотрудничество с внутренними заинтересованными сторонами и внешними организациями.

Цель состоит в повышении уровня безопасности в организации, а также в повышении значимости безопасности для организации, с тем чтобы способствовать дальнейшему ее развитию и укреплению.

На рисунке 8 показаны категории услуг и соответствующие им процессы управления, а в таблице 4 приведен перечень услуг.

Подробное описание каждой услуги из перечня услуг CDC приведено в Приложении A.

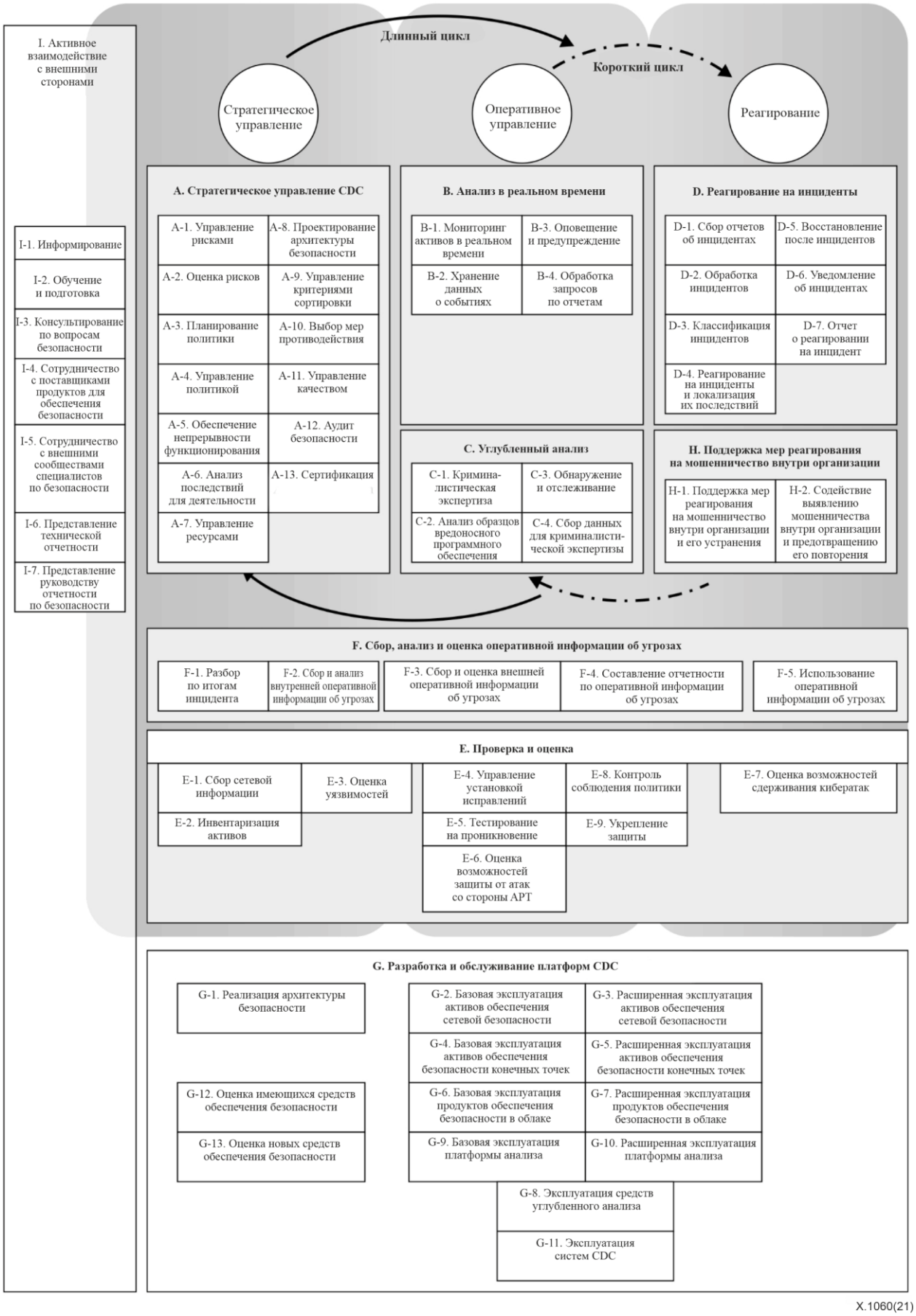

Рисунок 8 – Категории услуг CDC

Таблица 4 – Перечень услуг CDC

A	**Стратегическое управление CDC**
A-1	Управление рисками
A-2	Оценка рисков
A-3	Планирование политики
A-4	Управление политикой
A-5	Обеспечение непрерывности функционирования
A-6	Анализ последствий для деятельности
A-7	Управление ресурсами
A-8	Проектирование архитектуры безопасности
A-9	Управление критериями сортировки
A-10	Выбор мер противодействия
A-11	Управление качеством
A-12	Аудит безопасности
A-13	Сертификация
B	**Анализ в реальном времени**
B-1	Мониторинг активов в реальном времени
B-2	Хранение данных о событиях
B-3	Оповещение и предупреждение
B-4	Обработка запросов по отчетам
C	**Углубленный анализ**
C-1	Криминалистическая экспертиза
C-2	Анализ образцов вредоносного программного обеспечения
C-3	Обнаружение и отслеживание
C-4	Сбор данных для криминалистической экспертизы
D	**Реагирование на инциденты**
D-1	Сбор отчетов об инцидентах
D-2	Обработка инцидентов
D-3	Классификация инцидентов
D-4	Реагирование на инциденты и локализация их последствий
D-5	Восстановление после инцидентов
D-6	Уведомление об инцидентах
D-7	Отчет о реагировании на инцидент
E	**Проверка и оценка**
E-1	Сбор сетевой информации
E-2	Инвентаризация активов
E-3	Оценка уязвимостей
E-4	Управление установкой исправлений
E-5	Тестирование на проникновение
E-6	Оценка возможностей защиты от атак со стороны APT
E-7	Оценка возможностей сдерживания кибератак
E-8	Контроль соблюдения политики
E-9	Укрепление защиты

F	**Сбор, анализ и оценка оперативной информации об угрозах**
F-1	Разбор по итогам инцидента
F-2	Сбор и анализ внутренней оперативной информации об угрозах
F-3	Сбор и оценка внешней оперативной информации об угрозах
F-4	Составление отчетности по оперативной информации об угрозах
F-5	Использование оперативной информации об угрозах
G	**Разработка и обслуживание платформ CDC**
G-1	Реализация архитектуры безопасности
G-2	Базовая эксплуатация активов обеспечения сетевой безопасности
G-3	Расширенная эксплуатация активов обеспечения сетевой безопасности
G-4	Базовая эксплуатация активов обеспечения безопасности конечных точек
G-5	Расширенная эксплуатация активов обеспечения безопасности конечных точек
G-6	Базовая эксплуатация продуктов обеспечения безопасности в облаке
G-7	Расширенная эксплуатация продуктов обеспечения безопасности в облаке
G-8	Эксплуатация средств углубленного анализа
G-9	Базовая эксплуатация платформы анализа
G-10	Расширенная эксплуатация платформы анализа
G-11	Эксплуатация систем CDC
G-12	Оценка имеющихся средств обеспечения безопасности
G-13	Оценка новых средств обеспечения безопасности
H	**Поддержка мер реагирования на мошенничество внутри организации**
H-1	Поддержка мер реагирования на мошенничество внутри организации и его устранения
H-2	Содействие выявлению мошенничества внутри организации и предотвращению его повторения
I	**Активное взаимодействие с внешними сторонами**
I-1	Информирование
I-2	Обучение и подготовка
I-3	Консультирование по вопросам безопасности
I-4	Сотрудничество с поставщиками продуктов для обеспечения безопасности
I-5	Сотрудничество с внешними сообществами специалистов по безопасности
I-6	Представление технической отчетности
I-7	Представление руководству отчетности по безопасности

Приложение A

Перечень услуг CDC с описаниями

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

A.1 Категория A. Стратегическое управление CDC

A.1.1 A-1. Управление рисками

Услуга по управлению рисками – обеспечение координации деятельности согласно пунктам A-2–A-13 по руководству и управлению организацией в части рисков.

A.1.2 A-2. Оценка рисков

Услуга по оценке рисков – определение уровня рисков организации по состоянию на текущий момент исходя из активов, угроз и мер по обеспечению безопасности.

A.1.3 A-3. Планирование политики

Услуга по планированию политики – поддержка всех мероприятий по выработке конкретной политики безопасности и составлению руководящих указаний.

A.1.4 A-4. Управление политикой

Услуга по управлению политикой – периодический пересмотр правил политики и регламентов организации для их оценки на предмет соответствия новым или внешним требованиям (например, нормативно-правовым актам и руководящим указаниям).

A.1.5 A-5. Обеспечение непрерывности функционирования

Услуга по обеспечению непрерывности функционирования – содействие выполнению оперативных функций, необходимых для надлежащей реализации и исполнения плана обеспечения непрерывности функционирования организации.

A.1.6 A-6. Анализ последствий для деятельности

Услуга по анализу последствий для деятельности – систематическая оценка возможных последствий различных событий или сценариев. Эта услуга помогает организациям оценить масштаб возможных потерь. В ходе анализа последствий могут рассматриваться не только прямые финансовые потери, но и другие последствия, например утрата доверия заинтересованных сторон и ущерб репутации.

A.1.7 A-7. Управление ресурсами

Услуга по управлению ресурсами – планирование ресурсов (персонала, бюджета, систем и т. д.) для поддержки мероприятий по обеспечению безопасности и выделение этих ресурсов для каждой услуги в надлежащем объеме и надлежащего качества.

A.1.8 A-8. Проектирование архитектуры безопасности

Услуга по проектированию архитектуры безопасности – создание архитектуры, которая позволит обеспечить безопасность деятельности организации. Разработка и обслуживание платформ CDC (категория G) может осуществляться путем сведения воедино различных требований по оценке безопасности, учитывающих структуру системы и ограничения бизнес-процессов (например, применительно к цепочкам поставок).

A.1.9 A-9. Управление критериями сортировки

Услуга по управлению критериями сортировки – установление конкретных критериев сортировки (приоритетного реагирования) в отношении событий (инцидентов, выявленных уязвимостей, полученной информации об угрозах) в согласованных рамках, определяемых общей политикой.

A.1.10 A-10. Выбор мер противодействия

Услуга по выбору мер противодействия – поддержка всей деятельности по выбору мер противодействия в соответствии с критериями сортировки (A-9), а также наилучших технологий, касающихся всех аспектов безопасности.

A.1.11 A-11. Управление качеством

Услуга по управлению качеством – выявление проблем в связи с качеством проводимых мероприятий по обеспечению безопасности независимо от того, оказывали ли они негативное воздействие на деятельность организации (например, на удобство пользования техническими средствами, производительность труда) за рассматриваемый период (например, за неделю или месяц).

A.1.12 A-12. Аудит безопасности

Услуга по аудиту безопасности – систематическая проверка количественных показателей реализации политики и мер безопасности в организации на конкретной площадке или в конкретное время. Персонал CDC участвует в аудите косвенным образом, предоставляя необходимую информацию и фактические данные о состоянии внедренных средств контроля.

A.1.13 A-13. Сертификация

Услуга по сертификации – поддержка мероприятий, обеспечивающих соблюдение организацией различных стандартов и схем сертификации.

A.2 Категория B. Анализ в реальном времени

A.2.1 B-1. Мониторинг активов в реальном времени

Услуга по мониторингу активов в реальном времени – контроль и анализ состояния систем или выявление и отслеживание подозрительных действий по журналам и данным наблюдения за сетевым трафиком, а также поддержка сортировки инцидентов или событий для сбора необходимой информации.

A.2.2 B-2. Хранение данных о событиях

Услуга по хранению данных о событиях – сбор и централизованное хранение информации о событиях, полученной в процессе мониторинга и анализа данных, касающихся безопасности.

A.2.3 B-3. Оповещение и предупреждение

Услуга по оповещению и предупреждению – уведомление соответствующих внутренних подразделений организации о событиях, которые составляют потенциальный риск для информационных активов (например, оповещения с устройств обеспечения безопасности, бюллетени по безопасности, уязвимости, распространяющиеся угрозы).

A.2.4 B-4. Обработка запросов по отчетам

Услуга по обработке запросов по отчетам – реагирование на запросы о данных и отчетах о результатах анализа.

A.3 Категория C. Углубленный анализ

A.3.1 C-1. Криминалистическая экспертиза

Услуга по криминалистической экспертизе – анализ цифровых данных, связанных с тем или иным событием и собранных с помощью активов по обеспечению безопасности, с целью выяснить, что произошло.

A.3.2 C-2. Анализ образцов вредоносного программного обеспечения

Услуга по анализу образцов вредоносного программного обеспечения – проведение анализа вредоносных программ и скриптов, развернутых злоумышленниками и обнаруженных в ходе каждой криминалистической экспертизы.

A.3.3 C-3. Обнаружение и отслеживание

Эта услуга характеризуется способностью организации обнаруживать и отслеживать источники всех атак на объекты ее инфраструктуры, что является решающим фактором предотвращения и сокращения числа будущих инцидентов безопасности. Подтвержденная способность обнаруживать и отслеживать внутренних и внешних злоумышленников (например, устанавливать авторство кибератак) может предотвратить новые атаки.

A.3.4 C-4. Сбор данных для криминалистической экспертизы

Услуга по сбору данных для криминалистической экспертизы – сбор и хранение цифровых электронных доказательств, связанных с рассматриваемым инцидентом, а также обеспечение достоверности этих доказательств (цепочка сохранения доказательств).

A.4 Категория D. Реагирование на инциденты

A.4.1 D-1. Сбор отчетов об инцидентах

Услуга по сбору отчетов об инцидентах – получение аналитических отчетов об операциях. Сюда может также относиться получение отчетов от другого подразделения организации или от внешней организации.

A.4.2 D-2. Обработка инцидентов

Услуга по обработке инцидентов – действия в отношении признанных инцидентов безопасности и координация мероприятий, включая услуги D-3–D-7.

A.4.3 D-3. Классификация инцидентов

Услуга по классификации инцидентов – отнесение инцидента к той или иной категории в целях выработки общего представления о видах и причинах возникающих инцидентов.

A.4.4 D-4. Реагирование на инциденты и локализация их последствий

Услуга по реагированию на инциденты и локализации их последствий – локализация инцидента, прежде чем он распространит свое воздействие на все ресурсы и причинит еще больший ущерб.

A.4.5 D-5. Восстановление после инцидентов

Услуга по восстановлению после инцидентов – содействие восстановлению нормального функционирования объекта системы.

A.4.6 D-6. Уведомление об инцидентах

Услуга по уведомлению об инцидентах – передача информации об инцидентах группе реагирования на инциденты, а также другим заинтересованным группам.

A.4.7 D-7. Отчет о реагировании на инцидент

Услуга по представлению отчета о реагировании на инцидент – составление и выпуск отчета о реагировании на обработанный инцидент (если меры противодействия затягиваются, отчет передается на уровень стратегического управления CDC (категория A)). Если персоналу CDC требуется отчет о текущем состоянии дел в ходе обработки инцидента, выпускается также промежуточный отчет.

A.5 Категория E. Проверка и оценка

A.5.1 E-1. Сбор сетевой информации

Услуга по сбору сетевой информации – обзор конфигурации сетей, подлежащих защите.

A.5.2 E-2. Инвентаризация активов

Услуга по инвентаризации активов – управление информацией, относящейся к переписи систем, активов и приложений, образующих бизнес-инфраструктуру, которая находится в сфере ведения CDC.

A.5.3 E-3. Оценка уязвимостей

Услуга по оценке уязвимостей – исследование сетей, систем и приложений для выявления уязвимостей, определения возможности их эксплуатации и выдачи рекомендаций по снижению соответствующих рисков.

A.5.4 E-4. Управление установкой исправлений

Услуга по управлению установкой исправлений – поддержка установки всех необходимых исправлений, связанных с безопасностью, при поддержании эксплуатационной готовности ИТ-служб.

A.5.5 E-5. Тестирование на проникновение

Услуга по тестированию на проникновение – выявление уязвимостей в системе безопасности, которые могут быть использованы злоумышленниками, и возможных методов нарушения безопасности (например, тестирования, выполняемого в ответ на полученную информацию об угрозах).

A.5.6 E-6. Оценка возможностей защиты от атак со стороны APT

Услуга по оценке возможностей защиты от атак, связанных с устойчивыми угрозами нового уровня (APT), – оценка устойчивости организации по отношению к целенаправленным атакам с проведением адресного инструктажа по безопасной работе с электронной почтой и тестов на противодействие психологическим атакам.

A.5.7 E-7. Оценка возможностей сдерживания кибератак

Услуга по оценке возможностей сдерживания кибератак – проверка того, возможно ли будет в реальности инициировать мероприятия по реагированию в случае атаки и без промедления урегулировать инцидент (этот процесс называется учениями по реагированию на кибератаки).

A.5.8 E-8. Контроль соблюдения политики

Услуга по контролю соблюдения политики – поддержка проверки соответствия установленной политике безопасности и ее соблюдения.

A.5.9 E-9. Укрепление защиты

Услуга по укреплению защиты – оптимизация конфигураций ИТ-компонентов для определения, оценки и применения конфигураций безопасности систем, а также для снижения или устранения рисков атак.

A.6 Категория F. Сбор, анализ и оценка оперативной информации об угрозах

A.6.1 F-1. Разбор по итогам инцидента

Услуга разбора по итогам инцидента – описание хода разрешения инцидента в целях пересмотра и совершенствования процессов и инструментов, которыми располагает персонал CDC.

A.6.2 F-2. Сбор и анализ внутренней оперативной информации об угрозах

Услуга по сбору и анализу внутренней оперативной информации об угрозах – сбор оперативной информации (внутренних оперативных данных) об анализе в реальном времени и реагировании на инциденты.

A.6.3 F-3. Сбор и оценка внешней оперативной информации об угрозах

Услуга по сбору и оценке внешней оперативной информации об угрозах – сбор оперативной информации (внешних оперативных данных), например о новых уязвимостях, тенденциях кибератак, поведении вредоносного программного обеспечения и вредоносных IP-адресах или доменах.

A.6.4 F-4. Составление отчетности по оперативной информации об угрозах

Услуга по составлению отчетности по оперативной информации об угрозах – сбор и подробная документальная регистрация всей информации о внутренних и внешних угрозах.

A.6.5 F-5. Использование оперативной информации об угрозах

Услуга по использованию оперативной информации об угрозах – сведение воедино и распространение информации об угрозах по всем категориям реагирования.

A.7 Категория G. Разработка и обслуживание платформ CDC

A.7.1 G-1. Реализация архитектуры безопасности

Услуга по реализации архитектуры безопасности – внедрение архитектуры безопасности, спроектированной на уровне стратегического управления CDC (категория A), с использованием активов.

A.7.2 G-2. Базовая эксплуатация активов обеспечения сетевой безопасности

Услуга по базовой эксплуатации активов обеспечения сетевой безопасности – эксплуатация сетевых устройств, таких как брандмауэры, системы обнаружения и предотвращения вторжений (IDS/IPS), брандмауэры веб-приложений (WAF) и прокси-серверы.

A.7.3 G-3. Расширенная эксплуатация активов обеспечения сетевой безопасности

Услуга по расширенной эксплуатации активов обеспечения сетевой безопасности – создание собственных сигнатур организации для продуктов с возможностями обнаружения атак (IDS/IPS, WAF), а также их применение в случаях, когда сигнатур от поставщиков оказывается недостаточно.

A.7.4 G-4. Базовая эксплуатация активов обеспечения безопасности конечных точек

Услуга по базовой эксплуатации активов обеспечения безопасности конечных точек – эксплуатация продуктов, например антивирусного программного обеспечения, для противодействия атакам в конечных точках.

A.7.5 G-5. Расширенная эксплуатация активов обеспечения безопасности конечных точек

Услуга по расширенной эксплуатации активов обеспечения безопасности конечных точек – выявление подозрительных действий программ в конечных точках с использованием соответствующих продуктов для их защиты, а также сбор и анализ данных о состоянии реестров, выполнении процессов и т. д. При необходимости сюда может входить также выработка собственных показателей нарушения безопасности конечных точек.

A.7.6 G-6. Базовая эксплуатация продуктов обеспечения безопасности в облаке

Услуга по базовой эксплуатации продуктов обеспечения безопасности в облаке – эксплуатация служб безопасности в облачной среде.

A.7.7 G-7. Расширенная эксплуатация продуктов обеспечения безопасности в облаке

Услуга по расширенной эксплуатации продуктов обеспечения безопасности в облаке – создание собственных сигнатур для служб безопасности в облачной среде с возможностями обнаружения атак. Если предоставленных поставщиком сигнатур недостаточно, применяются собственные сигнатуры организации.

A.7.8 G-8. Эксплуатация средств углубленного анализа

Услуга по эксплуатации средств углубленного анализа – эксплуатация средств, используемых для углубленного анализа, например для цифровой криминалистической экспертизы и анализа вредоносного программного обеспечения.

A.7.9 G-9. Базовая эксплуатация платформы анализа

Услуга по базовой эксплуатации платформы анализа – эксплуатация аналитической инфраструктуры, обеспечивающей хранение требуемых данных из журналов и их анализ на постоянной основе (главным образом анализ в реальном времени), например систем управления информацией о безопасности и администрирования событий (SIEM).

A.7.10 G-10. Расширенная эксплуатация платформы анализа

Услуга по расширенной эксплуатации платформы анализа – более подробный и точный анализ с использованием собственных систем организации для ведения журналов и регистрации сетевых пакетов в объеме и составе, не обеспечиваемых коммерческими SIEM-системами, а также разработка собственных алгоритмов анализа и логики обработки этих данных наряду с соответствующими системами.

A.7.11 G-11. Эксплуатация систем CDC

Услуга по эксплуатации систем CDC – эксплуатация систем, выполняющих необходимые задачи реагирования, такие как использование описанных выше средств реагирования, составление различных отчетов, обработка запросов и управление уязвимостями.

A.7.12 G-12. Оценка имеющихся средств обеспечения безопасности

Услуга по оценке имеющихся средств обеспечения безопасности – проверка того, каким образом модернизация или изменение настроек имеющихся средств обеспечения безопасности повлияют на другие системы и виды деятельности (главным образом в смысле эксплуатационной готовности).

A.7.13 G-13. Оценка новых средств обеспечения безопасности

Услуга по оценке новых средств обеспечения безопасности – проектирование и развертывание новых активов для обеспечения безопасности, если возникла необходимость в принятии новых мер безопасности.

A.8 Категория H. Поддержка мер реагирования на мошенничество внутри организации

A.8.1 H-1. Поддержка мер реагирования на мошенничество внутри организации и его устранение

Услуга по поддержке мер реагирования на мошенничество внутри организации и его устранение – поддержка действий организации по реагированию на выявленное внутреннее мошенничество путем восстановления картины происшедшего по данным из журналов, собранным в рамках мероприятий по обеспечению безопасности.

A.8.2 H-2. Содействие выявлению мошенничества внутри организации и предотвращению его повторения

Услуга по содействию выявлению мошенничества внутри организации и предотвращению его повторения – подробный анализ выявленных внутренних мошеннических действий, рассмотрение возможности обнаружения таких действий по данным из журналов и реализация соответствующей логики, в случае если обнаружение признано возможным.

A.9 Категория I. Активное взаимодействие с внешними сторонами

A.9.1 I-1. Информирование

Услуга по информированию – предоставление соответствующим сотрудникам точной информации о CDC и связанных с ним вопросах, а также содействие применению правильных инструментов, передового опыта, надлежащей политики и ресурсов для защиты бизнес-активов организации.

A.9.2 I-2. Обучение и подготовка

Услуга по обучению и подготовке – поддержка мероприятий по специальной подготовке в области безопасности для сотрудников организаций, поддерживаемых CDC.

A.9.3 I-3. Консультирование по вопросам безопасности

Услуга по консультированию по вопросам безопасности – предоставление различным подразделениям организации консультаций по вопросам безопасности.

A.9.4 I-4. Сотрудничество с поставщиками продуктов для обеспечения безопасности

Услуга по сотрудничеству с поставщиками продуктов для обеспечения безопасности – установление прямой линии связи с поставщиком приобретенного продукта или услуги для обеспечения безопасности, запрос отклика на сообщения об обнаруженных в продукте или услуге недостатках и обмен конструктивными отзывами о возможных направлениях совершенствования.

A.9.5 I-5. Сотрудничество с внешними сообществами специалистов по безопасности

Услуга по сотрудничеству с внешними сообществами специалистов по безопасности – обеспечение заблаговременного обмена информацией путем участия во внешних сообществах. Такая информация может отражаться на мероприятиях организации по обеспечению безопасности.

A.9.6 I-6. Представление технической отчетности

Услуга по представлению технической отчетности – выпуск отчетов о результатах мониторинга и управления. Такие отчеты помогают оценить уровень безопасности систем и ИТ-инфраструктуры организации.

A.9.7 I-7. Представление руководству отчетов по безопасности

Услуга по представлению руководству отчетов по безопасности – периодическое представление высшему руководству отчетов и данных статистического анализа, отражающих уровень безопасности организации и показатели эффективности ее деятельности.

Библиография

[b-ITU-T X.1053] Recommendation ITU-T X.1053 (2017), *Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.