Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1604

(03/2020)

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

Безопасность облачных вычислений –
Проектирование безопасности облачных вычислений

Требования безопасности к сети как услуге (NaaS) в среде облачных вычислений

Рекомендация МСЭ-Т X.1604

Международный союз электросвязи

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.1379
Безопасность технологии распределения реестра	X.1400–X.1429
Безопасность технологии распределения 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	X.1700–X.1729

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

Рекомендация МСЭ-Т X.1604

Требования безопасности к сети как услуге (NaaS) в среде облачных вычислений

Резюме

В Рекомендации МСЭ-Т X.1604 приведен анализ угроз и проблем безопасности сети как услуги (NaaS) в среде облачных вычислений и определены требования безопасности NaaS для приложения NaaS, платформы NaaS и связности NaaS на основе соответствующих типов облачных возможностей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1604	26.03.2020 г.	17-я	11.1002/1000/14093

Ключевые слова

Облако, сеть как услуга, требования безопасности.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите 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 Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1604

Требования безопасности к сети как услуге (NaaS) в среде облачных вычислений

1 Сфера применения

В настоящей Рекомендации приведен анализ угроз и проблем безопасности сети как услуги (NaaS) в среде облачных вычислений и определены требования безопасности NaaS для приложения NaaS, платформы NaaS и связности NaaS на основе соответствующих типов облачных возможностей.

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 статуса Рекомендации.

[ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 г.), *Основы безопасности облачных вычислений.*

[ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 г.) | ИСО/МЭК 17788:2014, *Информационные технологии – Облачные вычисления – Обзор и терминология.*

[ITU-T Y.3512] Рекомендация МСЭ-Т Y.3512 (2014 г.), *Облачные вычисления – функциональные требования к сети как услуге.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 управление доступом (access control) [b-ITU-T X.800]: Предотвращение несанкционированного использования ресурса, в том числе предотвращение использование ресурса несанкционированным способом.

3.1.2 аутентификация (authentication) [b-ISO/IEC 18014-2]: Обеспечение гарантии идентичности объекта.

3.1.3 авторизация (authorization [b-ITU-T X.1251]: Услуга авторизации предназначена для того, чтобы принимать решения о правах доступа пользователя и обеспечивать исполнение решений об авторизации согласно привилегиям пользователя. Авторизация представляет собой дополнительную услугу; она предоставляется только в том случае, когда необходимо управление доступом к ресурсам на основании прав пользователя.

3.1.4 конфиденциальность (confidentiality) [b-ITU-T X.800]: Свойство, защищающее информацию от доступа к ней или ее раскрытия неуполномоченными лицами, объектами или процессами.

3.1.5 целостность данных (data integrity) [b-ITU-T X.800]: Показатель того, что данные не были изменены или разрушены несанкционированным способом.

3.1.6 брандмауэр (firewall) [b-ISO/IEC 27033-1]: Вид барьера безопасности, размещаемого между различными сетевыми средами, который состоит из специализированного устройства или совокупности нескольких компонентов и технических приемов и через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности.

3.1.7 система обнаружения вторжений (intrusion detection system) [b-ISO/IEC 27039]: Информационные системы, используемые для выявления попыток вторжения, совершаемых или совершенных вторжений.

3.1.8 ключ (key) [b-ITU-T X.800]: Последовательность символов, которая управляет операциями шифрования и дешифрования.

3.1.9 управление ключами (key management) [b-ITU-T X.800]: Генерирование, хранение, распределение, удаление, архивирование и применение ключей в соответствии со стратегией безопасности.

3.1.10 сертификат открытого ключа (public-key certificate, PKC) [b-ITU-T X.509]: Открытый ключ объекта в совокупности с некоторой дополнительной информацией, подделка которого исключена благодаря цифровой подписи с закрытым ключом органа по сертификации (CA), который его выдал.

3.1.11 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

BoD	Bandwidth on Demand	Пропускная способность по требованию
CSC	Cloud Service Customer	Потребитель облачной услуги
CSP	Cloud Service Provider	Поставщик облачной услуги
DDoS	Distributed Denial of Service	Распределенная атака типа "отказ в обслуживании"
DoS	Denial of Service	Отказ в обслуживании
NaaS	Network as a Service	Сеть как услуга
SNMP	Simple Network Management Protocol	Простой протокол управления сетью
vCDN	virtual Content Delivery Network	Виртуальная сеть доставки контента
vEPC	virtualized Evolved Packet Core	Виртуализированное улучшенное ядро пакетной сети
vFW	virtual Firewall	Виртуальный брандмауэр
VPN	Virtual Private Network	Виртуальная частная сеть

5 Соглашения

В настоящей Рекомендации:

ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым, таким образом для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

ключевое слово "**запрещается**" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевые слова "**может факультативно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации

поставщика должен обеспечивать выполнение этой функции и функция может быть активирована по желанию оператора сети/поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей Рекомендации.

6 Обзор

В [ITU-T Y.3500] категория облачной услуги определена как группа облачных услуг, обладающих некоторым общим набором характеристик качества. Сеть как услуга (NaaS) – это одна из категорий облачных услуг, в которой возможностью, предоставляемой потребителю облачной услуги (CSC), является возможность транспортного соединения и связанные с ним сетевые возможности.

Согласно [ITU-T Y.3512] услуги NaaS могут обеспечивать любую из следующих трех типов облачных возможностей: услуга приложения NaaS, услуга платформы NaaS и услуга связности NaaS.

- **Услуга приложения NaaS** предоставляет для CSC облачное сетевое приложение, такое, например, как виртуальный маршрутизатор, виртуальная сеть доставки контента (vCDN), виртуализированное улучшенное ядро пакетной сети (vEPC) и виртуальный брандмауэр (vFW).
- **Услуга платформы NaaS** предоставляет для CSC сетевую платформу, которая обеспечивает программируемую среду для сетевых функциональных средств.
- **Услуга связности NaaS** выполняет для CSC инициализацию и использует ресурсы сетевой связности, такие как гибкая и расширенная виртуальная частная сеть (VPN), пропускная способность по требованию (BoD) и т. д.

Концепция высокого уровня NaaS может быть описана согласно рисунку 1:

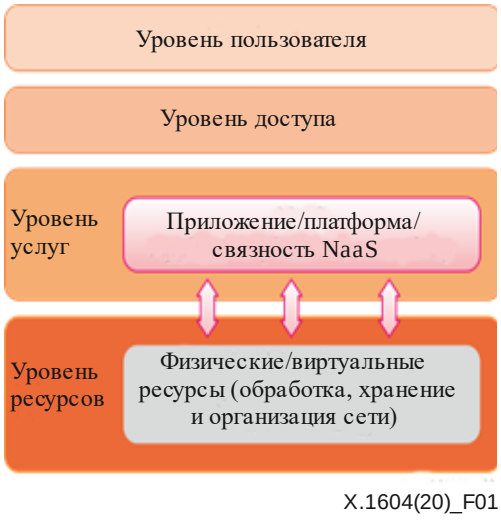

Рисунок 1 – Концепция высокого уровня NaaS

Используя эти три вида сетевых услуг, NaaS может обеспечивать сетевые функции в среде облачных вычислений, в том числе: координирование виртуализации вычислений и хранения с сетевыми возможностями, согласованное управление разнородными сетевыми технологиями, реконфигурацию по требованию.

С другой стороны, в NaaS необходимо решить ряд задач обеспечения безопасности.

- **Угрозы и проблемы безопасности в приложении NaaS**: услуга приложения NaaS должна обеспечивать для CSC посредством CSP предоставление приложений виртуальной сети, таких как виртуальный брандмауэр (vFW), виртуальный маршрутизатор, виртуальная сеть доставки (vCDN) и т. д. Услуга приложения NaaS должна решать проблемы безопасности, обусловливаемые уязвимостями защиты приложения, рисками нарушения безопасности виртуализации сети, совместным использованием физических сетевых устройств и т. д.

- **Угрозы и проблемы безопасности платформы NaaS**: услуга платформы NaaS должна обеспечивать для CSC посредством CSP программную среду, а также платформу для управления, развертывания и выполнения сетевых приложений. К проблемам безопасности платформы NaaS относятся, в том числе атаки типа DoS на сетевых платформах, уязвимости защиты операционных систем, нарушение управления доступом и т. д.
- **Угрозы и проблемы безопасности связности NaaS**: услуга связности NaaS должна обеспечивать для CSC посредством CSP сетевое соединение, такое как виртуальная частная сеть (VPN), пропускная способность по требованию (BoD) и т. д. Проблема безопасности услуги связности создает риски не только для услуг NaaS, но также для других облачных ресурсов и данных CSC. К проблемам безопасности услуги связности NaaS относятся, в том числе подслушивание, атаки через посредника и т. д

В настоящей Рекомендации приведен анализ требований безопасности для NaaS в среде облачных вычислений, включая приложение NaaS, платформу NaaS и связность NaaS.

7 Угрозы и проблемы безопасности сети как услуги в среде облачных вычислений

В разделах 7 и 8 [ITU-T X.1601] описаны угрозы и проблемы безопасности CSC и CSP в среде облачных вычислений, соответственно. Для NaaS в облаке также возникают угрозы и проблемы безопасности, аналогичные описанным в [ITU-T X.1601], которые определены ниже:

a) системные уязвимости;

b) потеря и утечка данных;

c) незащищенный доступ к услуге;

d) несанкционированный административный доступ;

e) внутренние угрозы;

f) потеря доверия;

g) потеря управления;

h) потеря конфиденциальности;

i) неготовность услуги;

j) совместно используемая среда.

Каждая облачная возможность характеризуется для NaaS в среде облачных вычислений конкретными угрозами и проблемами безопасности.

7.1 Угрозы и проблемы безопасности приложения NaaS

a) Сетевые и системные уязвимости: злоумышленники могут использовать потенциальные уязвимости системы безопасности приложения NaaS. Технические дефекты виртуализации приложений NaaS могут создать риски нескольких видов, кроме того, неполностью проработанная технология эксплуатации и технического обслуживания может обусловить более серьезные риски.

b) Совместное использование физических сетевых устройств: в силу того, что сетевые устройства используются совместно, на одном из общих устройств вероятна потеря, утечка или неправомерное использование данных.

c) Незащищенный доступ: незащищенный доступ к приложению NaaS может вызвать потерю, утечку или неправомерное использование данных.

d) Несанкционированный административный доступ: несанкционированный административный доступ к приложению NaaS может привести к потере данных.

e) Уязвимости приложения: приложение NaaS может подвергаться атаке типа "отказ в обслуживании" (DoS) или распределенной атаке типа "отказ в обслуживании"; кроме того, атака может привести к повреждению оборудования и вызвать потерю или разрушение данных.

7.2 Угрозы и проблемы безопасности платформы NaaS

a) Атаки DoS на сетевую платформу: когда одна или несколько платформ поверглись атакам типа "отказ в обслуживании" (DoS), платформа или другие виртуализированные платформы не могут отвечать из-за потребления ресурсов центрального процессора и памяти.

b) Уязвимости защиты операционной системы: данные на платформе NaaS могут быть потеряны; кроме того, уязвимости защиты операционных систем могут привести к распространению вирусов или возникновению других серьезных рисков нарушения безопасности.

c) Нарушение управления доступом: нарушение управления доступом может вызвать потерю, утечку и неправомерное использование данных.

d) Неготовность сетевой платформы: неготовности платформы NaaS может привести к неготовности услуг NaaS, вследствие чего возможно ненадлежащее функционирование соответствующих приложений NaaS и связности NaaS.

e) Несанкционированный административный доступ: несанкционированный административный доступ к платформе NaaS может привести к потере, утечке или неправомерному использованию данных. Например, злоумышленники могут использовать уязвимость системы, для того чтобы получить несанкционированный административный доступ к платформе NaaS и изменить IP-адрес пункта сбора данных на IP-адрес злоумышленника.

f) Угрозы со стороны работников: если клиентом услуги NaaS является не отдельное физическое лицо, а компания или организация, работники организации могут совместно использовать пароли "администратора", которые может использовать и поставщик услуги NaaS. Неосторожные или недостаточно подготовленные пользователи (или члены семьи, входящие в ближайшее окружение потребителя) или злонамеренные действия недовольных работников всегда представляют собой существенную угрозу.

7.3 Угрозы и проблемы безопасности связности NaaS

a) Подслушивание: злоумышленники могут перехватывать данные соединения и данные передачи.

b) Атака на сетевое соединение: во время сетевого соединения могут происходить атаки на сеть, такие как атаки через посредника, атаки DoS и т. д.

c) Потеря и утечка данных: клиенты NaaS, пользуясь услугами NaaS, как правило используют предоставляемую поставщиками сеть для транспортирования данных. Эти данные могут содержать личную информацию, коммерческие секреты и сведения политического характера. Вследствие этого утечка данных составляет серьезную угрозу для пользователей NaaS.

d) Спуфинг: злоумышленники могут маскироваться под систему управления или сервер хранения данных NaaS в среде облачных вычислений, результатом чего может стать потеря данных соединения или передачи.

e) Взлом и перехват: поврежденное сетевое оборудование, проникновение хакера и банкротство поставщика услуг NaaS могут привести к потере данных без возможности восстановления. Наряду с этим хакеры, в случае успешного проникновения, могут также взломать данные.

f) Незащищенный доступ в сеть: незащищенный доступ в сеть может привести к потере, утечке или неправомерному использованию данных соединения или данных передачи.

g) Незащищенная аутентификация идентичности: незащищенная аутентификация идентичности может привести к потере, утечке или неправомерному использованию данных соединения или данных передачи.

h) Неготовность сети: сетевая связность NaaS может подвергаться атакам типа DoS или DDoS; кроме того, атаки DDoS могут вызвать выход из строя серверов NaaS в среде облачных вычислений.

i) Уязвимость интерфейса сбора данных: злоумышленники могут использовать процесс сбора данных мониторинга, для того чтобы эксплуатировать уязвимости интерфейса.

j) Несанкционированный административный доступ: несанкционированный административный доступ к системной связности NaaS может привести к потере данных передачи.

8 Требования безопасности для NaaS

В данном разделе определены требования безопасности для NaaS в среде облачных вычислений.

8.1 Требования безопасности для приложения NaaS

Ниже определены требования безопасности для приложения NaaS.

a) a) Требуется поддерживать целостность и точность данных приложения NaaS.

b) Рекомендуется обеспечить методы управления доступом к данным приложения NaaS, такие как белые списки, черные списки и т. д.

c) Рекомендуется, чтобы CSP обеспечивал для CSC надлежащие методы управления доступом, такие как белые/черные списки, учетная запись и пароль и т. д., для того чтобы предотвратить доступ неавторизованных пользователей к системам или данным. Общие решения управления доступом для среды облачных вычислений приведены в [ITU-T X.1601].

d) Требуется, чтобы CSP поддерживал ведение журнала и аудит использования приложения NaaS.

e) Требуется, чтобы CSP поддерживал средства защиты от системных уязвимостей приложения NaaS; например, для того чтобы предотвратить системные уязвимости приложений NaaS, CSP может использовать методы тестирования на проникновение.

f) Требуется, чтобы CSP поддерживал методы резервного копирования, для того чтобы предотвратить потерю данных приложения NaaS, например резервное копирование с использованием физических дисков, методы распределенного хранения данных и т. д. Общие методы резервного копирования описаны в [ITU-T X.1601].

В таблице 8-1 представлено преобразование угроз безопасности приложения NaaS в требования безопасности для приложения NaaS.

Таблица 8-1 – Приложение NaaS: преобразование угроз безопасности в требования безопасности

Угрозы безопасности	Требования безопасности
Уязвимости безопасности приложения	b), d), e), f)
Риски нарушения безопасности виртуализации сети	a), b), c), d), f)
Совместное использование физических сетевых устройств	a), b), c), d), f)
Незащищенный доступ	b), c), d), e), f)
Несанкционированный административный доступ	b), c), d), f)
Неготовность приложения	d), e), f)

8.2 Требования безопасности для платформы NaaS

Ниже определены требования безопасности для платформы NaaS.

a) Требуется поддерживать целостность и точность данных платформы NaaS.

b) Рекомендуется обеспечить методы управления доступом к данным платформы NaaS, такие как белые списки, черные списки и т. д.

c) Рекомендуется, чтобы CSP обеспечивал для CSC надлежащие методы управления доступом, такие как белые/черные списки, учетная запись и пароль и т. д., для того чтобы предотвратить доступ неавторизованных пользователей к системам или данным. Общие решения управления доступом для среды облачных вычислений приведены в [ITU-T X.1601].

d) Требуется, чтобы CSP поддерживал ведение журнала и аудит использования платформы NaaS.

e) Требуется, что CSP поддерживал средства защиты от системных уязвимостей платформы NaaS; например, для того чтобы предотвратить системные уязвимости приложений NaaS, CSP может использовать методы тестирования на проникновение.

f) Требуется, чтобы CSP поддерживал методы резервного копирования, для того чтобы предотвратить потерю данных платформы NaaS, например резервное копирование с использованием физических дисков, методы распределенного хранения данных и т. д. Общие методы резервного копирования описаны в [ITU-T X.1601].

В таблице 8-2 представлено преобразование угроз безопасности платформы NaaS в требования безопасности для платформы NaaS.

Таблица 8-2 – Платформа NaaS: преобразование угроз безопасности в требования безопасности

Угрозы безопасности	Требования безопасности
Атаки типа DoS на сетевую платформу	a), b), c), d), e), f)
Уязвимости зашиты операционной системы	a), b), d), e), f)
Нарушение управления доступом	a), b), c), d), e), f)
Неготовность сетевой платформы	a), d), e), f)
Несанкционированный административный доступ	b), c), d), f)
Угрозы со стороны работников	b), d), f)

8.3 Требования безопасности для связности NaaS

Ниже определены требования безопасности для связности NaaS.

a) Требуется поддерживать целостность и точность данных связности NaaS.

b) Рекомендуется обеспечить методы управления доступом к интерфейсам связности NaaS, такие как белые/черные списки и т. д.

c) Рекомендуется обеспечить криптографические методы для защиты данных соединения и передачи.

d) Рекомендуется использоваться стандартные сетевые протоколы между облачными ресурсами и серверами связности NaaS, например простой протокол управления сетью (SNMP) или другие стандартные сетевые протоколы.

e) Рекомендуется, чтобы CSP обеспечивал для CSC надлежащие методы управления доступом, такие как белые/черные списки, учетная запись и пароль и т. д., для того чтобы предотвратить доступ неавторизованных пользователей к системам или данным. Общие решения управления доступом для среды облачных вычислений описаны в [ITU-T X.1601].

f) Требуется, чтобы CSP поддерживал ведение журнала и аудит использования связности NaaS.

g) Требуется, чтобы CSP реализовал методы аутентификации в целях защиты доступа к данным связности NaaS, например двухфакторную аутентификацию или иные методы. Общие методы аутентификации для среды облачных вычислений приведены в [ITU-T X.1601].

h) Требуется, что CSP поддерживал средства защиты от системных уязвимостей связности NaaS. Например, для того чтобы предотвратить системные уязвимости связности NaaS, CSP может использовать методы тестирования на проникновение.

В таблице 8-3 представлено преобразование угроз безопасности связности NaaS в требования безопасности для связности NaaS.

Таблица 8-3 – Связность NaaS: преобразование угроз безопасности в требования безопасности

Угрозы безопасности	Требования безопасности
Подслушивание	b), c), d), e), f), g) h)
Атака на сетевое соединение	d), f), h)
Потеря и утечка данных	a), b), c), d), e), f), g) h)
Спуфинг	a), b), d), e), f), g) h)
Взлом и перехват	a), b), c), d), e), f), g) h)
Незащищенный доступ в сеть	b), c), d), e), f), g) h)
Незащищенная аутентификация личности	b), c) , e), f), g) h)
Неготовность сети	d), f), h)
Уязвимость интерфейса сбора данных	a), b), c), d), f), h)
Несанкционированный административный доступ	c), f), g)

Библиография

[b-ITU-T E.409] Рекомендация МСЭ-Т E.409 (2004 г.), *Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.) | ИСО/МЭК 7498-2:1989, *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТ*.

[b-ITU-T X.810] Рекомендация МСЭ-Т X.810 | ИСО/МЭК 10181-1:1995, *Информационная технология. Взаимосвязь открытых систем. Структуры безопасности для открытых систем: Обзор*.

[b-ITU-T X.1251] Рекомендация МСЭ-Т X.1251 (2019 г.), *Сценарии использования структурированного представления информации об угрозах*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19440] ИСО/МЭК 19440:2007, *Интеграция предприятия. Конструкции для моделирования*.

[b-ISO/IEC 19944] ISO/IEC 19944:2017, *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ИСО/МЭК 20000-1:2011, *Информационная технология (ИТ). Управление услугами. Часть 1. Требования к системе управления услугами*.

[b-ISO/IEC 27000] ИСО/МЭК 27000:2018, *Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология*.

[b-ISO/IEC 27033-1] ИСО/МЭК 27033-1:2015, *Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции*.

[b-ISO/IEC 27039] ИСО/МЭК 27039:2015, *Информационная технология. Методы защиты. Выбор, применение и операции систем обнаружения вторжений (IDPS)*.

[b-ISO/IEC 27729] ИСО/МЭК 27729:2012, *Информация и документация. Международный идентификатор стандартных наименований (ISNI)*.

[b-ISO/IEC 29100] ИСО/МЭК 29100:2011, *Информационная технология (ИТ). Методы и средства обеспечения безопасности. Основы обеспечения приватности*.

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, 2020 г.