Международный союз электросвязи

МСЭ-Т X.1601

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2014)

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

Безопасность облачных вычислений – Обзор безопасности облачных вычислений

Основы безопасности облачных вычислений

Рекомендация МСЭ-Т X.1601

ITU-T

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	
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	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	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
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

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

Рекомендация МСЭ-Т X.1601

Основы безопасности облачных вычислений

Резюме

В Рекомендации МСЭ-Т X.1601 изложены основы безопасности облачных вычислений. В Рекомендации проводится анализ угроз и проблем безопасности в среде облачных вычислений и приводится описание возможностей обеспечения безопасности, позволяющих смягчать последствия этих угроз и решать проблемы безопасности. Представлена базовая методика определения тех возможностей обеспечения безопасности, для которых потребуется спецификация в целях смягчения последствий угроз безопасности и решения проблем безопасности облачных вычислений. В Дополнении I приводится таблица соответствия, по которой определяется, как конкретная угроза или проблема безопасности разрешается с помощью одной или нескольких соответствующих возможностей обеспечения безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1601	24.01.2014 г.	17-я	11.1002/1000/12036-en

Ключевые слова

Облачные вычисления, защита конфиденциальности, возможности обеспечения безопасности, проблемы безопасности, основы безопасности, угрозы безопасности.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора 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 с целью 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

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
3.1	Термины, определенные в других документах	1
3.2	Термины, определенные в настоящей Рекомендации	2
4	Сокращения и акронимы	3
5	Соглашения по терминологии	4
6	Обзор	4
7	Угрозы безопасности облачных вычислений	5
7.1	Угрозы безопасности для потребителей облачной услуги (CSC)	5
7.2	Угрозы безопасности для поставщиков облачной услуги (CSP)	6
8	Проблемы безопасности облачных вычислений	7
8.1	Проблемы безопасности для потребителей облачной услуги (CSC)	7
8.2	Проблемы безопасности для поставщиков облачной услуги (CSP)	8
8.3	Проблемы безопасности для партнеров облачной услуги (CSN)	10
9	Возможности обеспечения безопасности облачных вычислений	11
9.1	Модель доверия	11
9.2	Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций	11
9.3	Физическая безопасность	12
9.4	Безопасность интерфейса	12
9.5	Безопасность виртуализации вычислений	12
9.6	Безопасность сети	12
9.7	Изолирование и защита данных и защита конфиденциальности	13
9.8	Координация обеспечения безопасности	13
9.9	Эксплуатационная безопасность	14
9.10	Управление инцидентами	14
9.11	Восстановительные работы при бедствиях	14
9.12	Оценка и аудит безопасности услуги	15
9.13	Функциональная совместимость, переносимость и обратимость	15
9.14	Безопасность цепи поставок	15
10	Базовая методика	16
Дополнение I – Соответствие угроз и проблем безопасности облачных вычислений возможностям обеспечения безопасности		19
Библиография		23

Рекомендация МСЭ-Т X.1601

Основы безопасности облачных вычислений

1 Сфера применения

В настоящей Рекомендации проводится анализ угроз и проблем безопасности в среде облачных вычислений и приводится описание возможностей обеспечения безопасности, позволяющих смягчать последствия этих угроз и решать проблемы безопасности. Представлена базовая методика определения тех возможностей обеспечения безопасности, для которых потребуется спецификация в целях смягчения последствий угроз безопасности и решения проблем безопасности облачных вычислений.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 аутентификация (authentication) [b-NIST-SP-800-53]: Проверка идентичности пользователя, процесса или устройства, нередко являющаяся необходимым условием обеспечения возможности доступа к ресурсам информационной системы.

3.1.2 возможность (capability) [b-ISO/IEC 19440]: Свойство, заключающееся в способности выполнять данный вид деятельности.

3.1.3 диспетчер персональных данных (data controller) [b-key definition]**:** Лицо, которое (либо самостоятельно, либо совместно или наряду с другими лицами) определяет, с какой целью и каким образом обрабатываются или должны обрабатываться любые персональные данные.

3.1.4 обработчик персональных данных (data processor) [b-key definition]: Применительно к персональным данным под этим понимается любое лицо (отличное от сотрудника оператора персональных данных), которое осуществляет обработку данных по поручению оператора персональных данных.

3.1.5 гипервизор (hypervisor) [b-NIST-SP-800-125]: Компонент виртуализации, осуществляющий управление гостевыми операционными системами (ОС) на хост-компьютере и контроль потоков инструкций между гостевыми ОС и физическим аппаратным обеспечением.

3.1.6 информация, позволяющая установить личность (personally identifiable information) [b-ISO/IEC 29100]: Любая информация, которая: a) может быть использована для идентификации субъекта PII, к которому такая информация относится; или b) прямо или косвенно связана либо может быть связана с субъектом PII.

3.1.7 домен безопасности (security domain) [b-ITU-T X.810]**:** Совокупность элементов, политика безопасности, орган обеспечения безопасности и набор связанных с безопасностью действий, в рамках которых к набору элементов применяется политика безопасности для указанных действий, а политикой безопасности управляет орган обеспечения безопасности для данного домена безопасности**.**

3.1.8 инцидент безопасности (security incident) [b-ITU-T E.409]: Инцидент безопасности – это любое неблагоприятное событие, в результате которого некий аспект безопасности может подвергнуться угрозе**.**

3.1.9 соглашение об уровне обслуживания (service level agreement (SLA)) [b-ISO/IEC 20000-1]**:** Документально оформленное соглашение между поставщиком услуги и потребителем, в котором определяются услуги и целевые показатели обслуживания**.**

ПРИМЕЧАНИЕ 1. – Соглашение об уровне обслуживания может заключаться также между поставщиком услуги и поставщиком, внутренней группой или потребителем, действующим в качестве поставщика.

ПРИМЕЧАНИЕ 2. – Соглашение об уровне обслуживания может быть включено в договор или в документально оформленное соглашение другого типа.

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

3.1.11 виртуальная машина (virtual machine (VM)) [b-NIST-SP-800-145]: Действующая изолированная логическая копия реальной машины.

3.1.12 уязвимость (vulnerability) [b-NIST-SP-800-30]: Слабое место информационной системы, процедур обеспечения безопасности системы, внутренних средств управления или реализации, которое может быть использовано источником угрозы.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 облачные вычисления (cloud computing): Парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу.

3.2.2 облачная услуга (cloud service): Одна или несколько возможностей, предоставляемых с использованием облачных вычислений (пункт 3.2.1), которые активируются с помощью заявленного интерфейса.

3.2.3 потребитель облачной услуги (cloud service customer): Сторона (пункт 3.2.12), которая состоит в деловых отношениях применительно к использованию облачных услуг (пункт 3.2.2).

3.2.4 партнер облачной услуги (cloud service partner): Партнер, участвующий в поддержке деятельности либо поставщика облачной услуги (пункт 3.2.5), либо потребителя облачной услуги (пункт 3.2.3) или же оказывает помощь в этой деятельности.

3.2.5 поставщик облачной услуги (cloud service provider): Сторона (пункт 3.2.12), которая предоставляет облачные услуги (пункт 3.2.2).

3.2.6 пользователь облачной услуги (cloud service user): Лицо, связанное с потребителем облачной услуги (пункт 3.2.3), которое пользуется облачными услугами (пункт 3.2.2).

3.2.7 связь как услуга (communications as a service (CaaS)): Категория облачной услуги, в которой возможностью, предоставляемой потребителю облачной услуги (пункт 3.2.3), является связь и взаимодействие в реальном времени.

ПРИМЕЧАНИЕ. – В CaaS могут предоставляться два типа возможностей: возможности платформы и возможности приложения.

3.2.8 коллективное облако (community cloud): Модель развертывания облака, которое обеспечивает исключительную поддержку конкретной группы потребителей облачной услуги (пункт 3.2.3) и совместно используется этой группой, при этом контроль ресурсов осуществляется как минимум одним членом этой группы.

ПРИМЕЧАНИЕ. – Общие требования включают, в том числе, миссию, требования к обеспечению безопасности, политику и задачи соблюдения правовых норм.

3.2.9 инфраструктура как услуга (infrastructure as a service (IaaS)): Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги (пункт 3.2.3), являются возможности инфраструктуры.

ПРИМЕЧАНИЕ. – Потребитель облачной услуги (пункт 3.2.3) не осуществляет контроль или управление в отношении внутренних физических или виртуальных ресурсов, но осуществляет контроль над операционными системами, запоминающими устройствами и развернутыми приложениями, которые используют физические и виртуальные ресурсы. Потребитель облачной услуги (пункт 3.2.3) может также иметь ограниченную возможность контроля над определенными компонентами сети (например, брандмауэрами хост-компьютеров).

3.2.10 множественная принадлежность (multi-tenancy): Распределение физических и виртуальных ресурсов, при котором несколько групп внутренних пользователей (пункт 3.2.18) и их вычисления и данные изолированы друг от друга и недоступны друг другу.

3.2.11 сеть как услуга (network as a service (NaaS)): Категория облачной услуги, в которой возможность, предоставляемая потребителю облачной услуги (пункт 3.2.3), относится к возможностям транспортного соединения и связанным с ним сетевым возможностям.

ПРИМЕЧАНИЕ. – В NaaS могут предоставляться любые из трех типов облачных возможностей.

3.2.12 сторона (party): Физическое лицо или организация.

3.2.13 платформа как услуга (platform as a service (PaaS)): Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю услуги (пункт 3.2.3), являются возможности платформы.

3.2.14 частное облако (private cloud): Модель развертывания облака, которое используется единственным потребителем облачной услуги (пункт 3.2.3), при этом контроль ресурсов осуществляется этим потребителем облачной услуги (пункт 3.2.3).

3.2.15 общественное облако (public cloud): Модель развертывания облака, которое теоретически доступно любому потребителю облачной услуги (пункт 3.2.3), при этом контроль ресурсов осуществляется поставщиком облачной услуги (пункт 3.2.5).

3.2.16 проблема безопасности (security challenge): Отличная от непосредственной угрозы безопасности "трудность", включающая "косвенные" угрозы, которая обусловлена характером и рабочей средой облачных услуг. См. пункты 7 и 8.

3.2.17 программное обеспечение как услуга (software as a service (SaaS)): Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги (пункт 3.2.3), являются возможности приложения.

3.2.18 группа внутренних пользователей (tenant): Группа пользователей облачной услуги (пункт 3.2.6), совместно использующих доступ к набору физических и виртуальных ресурсов.

ПРИМЕЧАНИЕ. – В контексте множественной принадлежности (пункт 3.2.10), как правило, группа пользователей облачной услуги (пункт 3.2.6), которая является группой внутренних пользователей, полностью относится к одной организации потребителя облачной услуги (пункт 3.2.3). Возможны случаи, когда группа пользователей облачной услуги (пункт 3.2.6) включает пользователей от нескольких различных потребителей, в частности в случае развертывания коллективного облака (пункт 3.2.8), но эти исключения являются особыми случаями. Вместе с тем в той или иной организации потребителей облачной услуги могут иметь место многие различные виды принадлежности при одном поставщике облачной услуги (пункт 3.2.5), возможно, представляющие различные деловые группы в рамках этой организации (например, службу продаж и бухгалтерию). Это связано с наличием объективных оснований, для того чтобы по деловым и коммерческим причинам обеспечить тщательное разнесение данных и видов деятельности, относящихся к этим разным группам.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Programming Interface		Интерфейс прикладного программирования
BCP	Business Continuity Plan		План обеспечения непрерывности деятельности
CaaS	Communications as a Service		Связь как услуга
CPU	Central Processing Unit	ЦП	Центральный процессор
CSC	Cloud Service Customer		Потребитель облачной услуги
CSN	Cloud Service Partner		Партнер облачной услуги
CSP	Cloud Service Provider		Поставщик облачной услуги
CSU	Cloud Service User		Пользователь облачной услуги
DNS	Domain Name System		Система наименований доменов
IaaS	Infrastructure as a Service		Инфраструктура как услуга
IAM	Identity and Access Management		Управление определением идентичности и доступом
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
IP	Internet Protocol		Протокол Интернет
IT	Information Technology	ИТ	Информационные технологии
NaaS	Network as a Service		Сеть как услуга

OS	Operating System	ОС	Операционная система
PaaS	Platform as a Service		Платформа как услуга
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
SaaS	Software as a Service		Программное обеспечение как услуга
SIM	Subscriber Identity Module		Модуль идентификации абонента
SLA	Service Level Agreement		Соглашение об уровне обслуживания
VM	Virtual Machine		Виртуальная машина

5 Соглашения по терминологии

Отсутствуют.

6 Обзор

Облачные вычисления – это парадигма обеспечения возможности удобного сетевого доступа по запросу к совместно используемому набору конфигурируемых ресурсов (например, сетям, серверам, запоминающим устройствам, приложениям и услугам), которые могут быть оперативно предоставлены и высвобождены при минимальном управленческом усилии или минимальном взаимодействии поставщиков услуг. Потребители услуг облачных вычислений могут использовать эти ресурсы для разработки, размещения и функционирования услуг и приложений по требованию и гибким образом на любом устройстве, в любое время и в любом месте в среде облачных вычислений. Услуги облачных вычислений, как правило, предоставляются в определенных категориях услуг, например инфраструктура как услуга (IaaS), платформа как услуга (PaaS), программное обеспечение как услуга (SaaS), сеть как услуга (NaaS) и т. д. Эти категории услуг позволяют потребителям услуг облачных вычислений быстро и легко начать или изменить свою деятельность, не создавая новую инфраструктуру и новые системы информационно-коммуникационных технологий (ИКТ), и обеспечивают возможность гибкого предоставления ресурсов в необходимом количестве. Например, некоторые поставщики облачных услуг (CSP) могут предоставлять удаленные ресурсы аппаратного и программного обеспечения, которые могут предлагаться как услуга (например, IaaS или NaaS). Другие поставщики облачных услуг могут предоставлять рассчитанные на облачную среду платформы (PaaS) или приложения (SaaS), позволяющие потребителям и партнерам быстро разрабатывать и внедрять новые приложения, которые могут настраиваться и использоваться дистанционно.

Внедрение облачных вычислений сопряжено с угрозами и проблемами безопасности, и требования к обеспечению безопасности существенно различаются для разных моделей развертывания услуг облачных вычислений и категорий услуг. Распределенный характер облачных вычислений, сопряженный с наличием нескольких групп внутренних пользователей, преобладание дистанционного доступа к услугам облачных вычислений и большое количество организаций, участвующих в каждом процессе, приводят к тому, что облачные вычисления изначально более уязвимы как к внутренним, так и внешним угрозам безопасности, нежели другие парадигмы. Многие угрозы безопасности могут быть уменьшены с применением традиционных процессов и механизмов обеспечения безопасности. Безопасность затрагивает многие составляющие услуг облачных вычислений и воздействует на них. В связи с этим одним из важнейших аспектов облачных вычислений является управление обеспечением безопасности услуг облачных вычислений, а также связанных с ними ресурсов.

Прежде чем переводить систему ИКТ в среду облачных вычислений потенциальному потребителю облачной услуги (CSC) следует выявить ее угрозы безопасности (см. пункт 7, ниже) и проблемы безопасности (см. пункт 8).

На основе этих угроз и проблем определяется набор высокоуровневых возможностей обеспечения безопасности (см. пункт 9). Конкретные требования к этим возможностям не входят в сферу применения настоящей Рекомендации, однако их потребуется определить для конкретных реализаций услуг облачных вычислений на основе оценки риска в зависимости от выявленных угроз и проблем.

На основе оценки риска CSC может определить, стоит ли внедрять облачные вычисления, а также принять обоснованные решения относительно поставщиков услуг и архитектуры. Указанную выше оценку риска следует осуществлять с помощью принципов управления рисками информационной безопасности (например, принципов управления рисками, определенных в [b-ISO/IEC 27005]). В отношении предполагаемой базовой методики см. также пункт 10, ниже.

В настоящей Рекомендации проводится различие между угрозами безопасности и проблемами безопасности. Угрозы безопасности – это угрозы, связанные с атаками (активными и пассивными), а также отказами под влиянием среды или бедствиями. Проблемы безопасности включают трудности, обусловленные характером и рабочей средой облачных услуг. Если надлежащим образом не решить проблемы безопасности, то могут возникнуть угрозы.

С учетом этих выявленных угроз и проблем безопасности приводится описание возможностей обеспечения безопасности, призванных уменьшить угрозы безопасности и решить проблемы безопасности облачных вычислений.

7 Угрозы безопасности облачных вычислений

Угрозы связаны с потенциальным ущербом ресурсам, например информации, процессам и системам, а значит, организациям. Угрозы могут иметь стихийное или антропогенное происхождение и быть случайными или намеренными. Угроза может возникнуть внутри или вне организации. Угрозы можно разделить на случайные или намеренные, а также активные или пассивные.

Конкретные обнаруженные угрозы сильно зависят от выбранной конкретной облачной услуги. Например, применительно к общественному облаку, угрозы могут возникнуть из-за разделения ответственности между CSC и CSP: сложности определения юрисдикции над данными и процессами, согласованность и адекватность защиты данных, обеспечение конфиденциальности и т. д. Вместе с тем в частном облаке устранить угрозы проще, потому что CSC осуществляет контроль над всеми группами внутренних пользователей хостинга, обеспечиваемого CSP. Несмотря на то, что некоторые из выявленных в настоящей Рекомендации угроз рассматриваются в существующих отраслевых документах (например, в Рекомендации МСЭ-Т X.800), все эти угрозы характерны для облачных вычислений. Актуальность отдельных угроз зависит от конкретной облачной услуги.

В настоящем пункте приводится описание различных угроз безопасности, которые могут возникать в среде облачных вычислений.

7.1 Угрозы безопасности для потребителей облачной услуги (CSC)

Приведенные ниже угрозы непосредственно затрагивают CSC. Они могут затрагивать личные или деловые интересы CSC, конфиденциальность, законность или безопасность. Не все CSC подвержены риску со стороны всех угроз. Риск не одинаков и зависит от характера CSC и используемой услуги облачных вычислений. Например, к облачной услуге, связанной с транскодированием коммерческих видеофайлов, не предъявляются требования по защите информации, позволяющей установить личность (PII), но к ней предъявляются серьезные требования, связанные с защитой цифровых ресурсов.

7.1.1 Потеря и утечка данных

В связи с тем, что в среде облачной услуги, как правило, существует несколько групп внутренних пользователей, потеря или утечка данных представляет серьезную угрозу для CSC. Отсутствие надлежащего управления криптографической информацией, например ключами шифрования, кодами аутентификации и правами доступа может нанести серьезный ущерб, например вызвать потерю данных или неожиданную утечку за пределы облака. Основными источниками этой угрозы могут считаться, например, недостаточные средства управления аутентификацией, авторизацией и аудитом, несогласованное использование ключей шифрования и/или аутентификации, эксплуатационные отказы, проблемы утилизации, вопросы юрисдикции и политические вопросы, надежность центров обработки данных и восстановление в случае бедствий, которые могут быть связаны с проблемами, описанными в пунктах 8.1.2 "Потеря доверия", 8.1.3 "Потеря управления" и 8.1.4 "Потеря конфиденциальности".

7.1.2 Незащищенный доступ к услуге

Регистрационные данные для определения идентичности, в том числе регистрационные данные администраторов CSC, особенно уязвимы перед неавторизованными пользователями в сильно распределенной среде облачных вычислений. Причина состоит в тот, что в отличие от традиционной электросвязи нередко бывает сложно использовать местоположение (например, телефон фиксированной связи) или наличие какого-либо конкретного элемента аппаратуры (например, модуля идентификации абонента (SIM) подвижной связи) для подтверждения аутентификации идентичности. В связи с тем, что большинство предлагаемых услуг являются дистанционными, незащищенные соединения оказываются потенциально уязвимыми. Даже в том случае, когда соединения защищены или являются местными, другие методы атак (например, фишинг, мошенничество, социальная инженерия и использование уязвимостей программного обеспечения) могут также оказаться успешными. Если злоумышленник получает доступ к регистрационным данным пользователя или администратора, он может перехватывать действия и транзакции, изменять данные, возвращать искаженную информацию и перенаправлять клиентские программы CSC на незаконные сайты. Одни и те же пароли нередко используются для нескольких веб-сайтов и услуг, что усиливает воздействие таких атак, поскольку в результате одного взлома незащищенными оказываются несколько услуг. Решения для облачных вычислений сопряжены в дополнительной угрозой, усугубляющей общую ситуация. Учетная запись CSC или экземпляры услуг могут стать для злоумышленника новой точкой опоры. В дальнейшем он может максимально использовать потенциал репутации и ресурсы CSC для осуществления последующих атак.

7.1.3 Внутренние угрозы

В случае участия человека всегда существует риск того, что действия отдельных лиц окажутся несовместимыми с обеспечением безопасности услуги. Сотрудники CSC, совместно использующие пароли администратора или иным образом оставляющие регистрационные данные незащищенными (например, написанными на листке, приклеенном к экрану), неосторожные или недостаточно подготовленные пользователи (или члены семьи, входящие в ближайшее окружение потребителя) или злонамеренные действия недовольных сотрудников всегда представляют собой угрозу.

7.2 Угрозы безопасности для поставщиков облачной услуги (CSP)

В настоящем пункте определяются угрозы, которые непосредственно затрагивают CSP. Такие угрозы могут затрагивать способность CSP предлагать услуги, осуществлять деятельность, удерживать клиентов и избегать правовых или регуляторных трудностей. Угрозы тому или иному CSP зависят и от его конкретного набора предлагаемых услуг и среды.

7.2.1 Несанкционированный административный доступ

Услуга облачных вычислений включает интерфейсы и компоненты программного обеспечения, позволяющие собственному персоналу CSC осуществлять административные функции в отношении тех аспектов услуг облачных вычислений, которые находятся под контролем CSC, таких как добавление или удаление учетных записей сотрудников CSC, подключение к собственным серверам CSC, изменение пропускной способности, обновление записей системы наименований доменов (DNS) и веб-сайтов и т. д. Подобные административные интерфейсы могут стать мишенью для злоумышленников, которые выдают себя за администраторов CSC, чтобы атаковать CSP. В связи с тем, что такие услуги облачных вычислений должны быть доступными собственному персоналу CSC, защита этих услуг становится одной из главных задач обеспечения безопасности облачных вычислений.

7.2.2 Внутренние угрозы

В случае участия человека всегда существует риск того, что вредоносные или неосторожные действия отдельных лиц подвергнут риску безопасность услуги.

Сотрудники CSC, совместно использующие пароли администратора, или иным образом оставляющие регистрационные данные незащищенными (например, написанными на листке, приклеенном к экрану), неосторожные или недостаточно подготовленные пользователи или злонамеренные действия недовольных сотрудников всегда представляют собой серьезную угрозу любой деятельности.

CSP необходимо особенно серьезно учитывать благонадежность своих собственных сотрудников. Даже при наличии эффективного предварительного отбора сотрудников всегда существует риск того, что опытные нарушители смогут получить должность сотрудника центра обработки данных CSP. Такие нарушители могут пытаться тайно навредить самому CSP, или же в их намерения может входить проникновение в конкретные поддерживаемые системы CSC, особенно если CSC является крупной корпорацией или правительственным учреждением.

8 Проблемы безопасности облачных вычислений

Проблемы безопасности включают отличные от непосредственной угрозы безопасности трудности, в том числе "косвенные" угрозы, которые обусловлены характером и рабочей средой облачных услуг. Косвенная угроза имеет место в том случае, если какая-либо угроза одному пользователю облачной услуги может иметь отрицательные последствия для других пользователей.

Определенные в настоящей Рекомендации проблемы являются проблемами, которые, не будучи решенными надлежащим образом, могут привести к возникновению угроз. Эти проблемы необходимо учитывать при рассмотрении услуг облачных вычислений.

8.1 Проблемы безопасности для потребителей облачной услуги (CSC)

В настоящем пункте приводится описание проблем безопасности, связанных со сложностями среды или косвенными угрозами, которые могут быть причиной более непосредственных угроз интересам CSC.

8.1.1 Неопределенность в отношении ответственности

Потребление предоставляемых ресурсов осуществляется CSC в рамках различных категорий услуг и моделей развертывания. Таким образом, создаваемая потребителем система ИКТ зависит от этих услуг. Любое отсутствие четко определенной ответственности между CSC и CSP может вызвать принципиальные или эксплуатационные конфликты. Любая несогласованность положений договора о предоставлении услуг может спровоцировать нарушения или инциденты. Например, на международном уровне может возникать проблема отсутствия четкого разделения того, какая структура является диспетчером персональных данных, а какая – обработчиком персональных данных, даже если международная составляющая сводится лишь к небольшой сторонней организации за пределами какого-либо конкретного региона, например Европейского союза.

Любая неясность, связанная с правовыми и регуляторными требованиями (например, является ли тот или иной CSC или CSP "диспетчером персональных данных" или "обработчиком персональных данных"), может привести к неопределенности в плане того, какой комплекс нормативных актов ему требуется соблюдать. Если данное толкование различно в разных юрисдикциях, на данный CSC или CSP могут распространяться противоречащие друг другу нормативные акты, касающиеся одной и той же услуги или части данных.

8.1.2 Потеря доверия

В некоторых случаях CSC трудно распознать уровень доверия своего CSP в связи с тем, что услуга облачных вычислений носит характер "черного ящика". В отсутствие средств получения информации об уровне доверия поставщика и обмена этой информацией формализованным образом у CSC отсутствуют средства оценки достигнутого поставщиком уровня реализации безопасности. Такое отсутствие обмена информацией на уровне безопасности касательно CSP может стать серьезной угрозой безопасности для некоторых CSC при использовании ими услуг облачных вычислений.

8.1.3 Потеря управления

Решение CSC о переводе части их собственной системы ИКТ на инфраструктуру облачных вычислений подразумевает передачу частичного контроля CSP. Такой шаг может стать серьезной угрозой для данных CSC, особенно применительно к присвоенной поставщику роли и привилегиям. В сочетании с отсутствием прозрачности в отношении методов работы поставщика услуг облачных вычислений это может привести к неправильной конфигурации или даже предоставить возможность злонамеренной внутренней атаки.

При внедрении услуг облачных вычислений у некоторых CSC может возникнуть обеспокоенность в связи с недостаточным контролем над собственной информацией и ресурсами, размещенными у CSP, в отношении хранения данных, надежности резервирования данных (вопросы сохранности данных), мер противодействия в планах обеспечения непрерывности деятельности (BCP), восстановительных работ при бедствиях и т. д.

Например:

- CSC хочет удалить файл по причинам правового характера, однако CSP сохраняет копию, о которой CSC не знает.
- CSP предоставляет привилегии администратора CSC, которые выходят за рамки политики CSC.
- У некоторых CSC может возникнуть обеспокоенность в связи с раскрытием CSP данных иностранным правительствам, что может повлиять на соблюдение CSC законов об охране конфиденциальности, например директив Европейского союза о защите данных.

8.1.4 Потеря конфиденциальности

При обработке CSP частной информации существует возможность нарушения конфиденциальности, которое не соответствует нормативным или законодательным актам об охране конфиденциальности. Сюда относится утечка частной информации или обработка частной информации в целях, которые не санкционированы CSC и/или субъектом данных.

8.1.5 Неготовность услуги

Готовность не связана исключительно со средой облачных вычислений. Однако в связи с принципом сервисно-ориентированного дизайна доставка услуг может оказаться затронутой в случае отсутствия полной готовности вышестоящих услуг облачных вычислений. Кроме того, динамическая зависимость облачных вычислений обеспечивает злоумышленникам более широкие возможности. Например, в той и той же системе облачных вычислений атака типа "отказ в обслуживании" на одну из вышестоящих услуг может затронуть несколько нижестоящих услуг.

8.1.6 Привязка к одному поставщику облачной услуги

Высокая зависимость от одного CSP может затруднить замену одного CSP другим. Такая ситуация может возникнуть в случае, когда CSP использует нестандартные функции или форматы и не обеспечивает функциональную совместимость. Если CSP, к которому осуществлена "привязка", не устраняет уязвимости в области безопасности, то может возникнуть угроза безопасности, и, таким образом, CSC оказывается уязвимым, но не имеет возможности перехода к другому CSP.

8.1.7 Неправомерное присвоение интеллектуальной собственности

В случае если CSP выполняет программный код или обеспечивает хранение других ресурсов CSC, существует проблема утечки этих материалов, которые могут попасть к третьим сторонам, или их неправомерного присвоения с целью несанкционированного использования. Сюда входит нарушение авторского права или раскрытие коммерческой тайны.

8.1.8 Потеря целостности программного обеспечения

Поскольку программный код CSC выполняется CSP, существует возможность изменения кода или его заражения вирусом, когда он выходит из-под непосредственного контроля CSC. Таким образом, это приводит к неправильному функционированию программного обеспечения CSC, проявляющемуся тем или иным образом. Несмотря на то что CSC не в состоянии проконтролировать данную возможность, она может серьезно затронуть его репутацию и, следовательно, его деятельность.

8.2 Проблемы безопасности для поставщиков облачной услуги (CSP)

В настоящем пункте приводится описание проблем безопасности, связанных со сложностями среды или косвенными угрозами, которые могут быть причиной более непосредственных угроз интересам CSP.

8.2.1 Неопределенность в отношении ответственности

В системе облачных вычислений могут быть определены разные роли (CSP, CSC и партнер облачной услуги (CSN)). Неопределенность в отношении определения ответственности, связанной с такими вопросами, как владение данными, контроль доступа или техническое обслуживание инфраструктуры, может отразиться на деловых или правовых спорах (особенно при взаимодействии со сторонними организациями, или если CSP является также CSC или CSN). Данный риск неопределенности увеличивается, если CSP эксплуатирует и/или предлагает услуги в нескольких юрисдикциях, где договоры и соглашения могут существовать на разных языках или основываться на разных нормативно-правовых базах. См. также п. 8.2.4 "Конфликт юрисдикций", ниже.

8.2.2 Совместно используемая среда

Облачные вычисления обеспечивают потенциальную экономию за счет совместного использования большого объема ресурсов, которое происходит в чрезвычайно большом масштабе. В данной ситуации незащищенными оказываются многие потенциально уязвимые интерфейсы. Например, различные CSC одновременно пользуются услугами из одного и того же облака. В результате CSC может теоретически получить несанкционированный доступ к виртуальным машинам, сетевому трафику, реальным/остаточным данным и прочим ресурсам других групп внутренних пользователей. Любой такой несанкционированный или злоумышленный доступ к ресурсам другого CSC может нарушить их целостность, готовность и конфиденциальность.

Например, несколько виртуальных машин, одновременно размещенных на одном физическом сервере, совместно используют центральный процессор (ЦП) и ресурсы памяти, которые виртуализуются гипервизором. В данном примере проблемы включают отказ механизмов изоляции гипервизора, при котором обеспечивается возможность несанкционированного доступа к памяти или устройствам хранения других виртуальных машин.

8.2.3 Несогласованность и конфликт механизмов защиты

В связи с децентрализованной архитектурой инфраструктуры облачных вычислений ее механизмы защиты могут быть несогласованными в разных распределенных модулях защиты. Например, доступ, запрещенный одним модулем безопасности, может быть предоставлен другим модулем. Такая несогласованность может создавать проблемы для авторизованного пользователя, и она может быть использована злоумышленником, и тем самым привести к нарушению конфиденциальности, целостности и готовности.

8.2.4 Конфликт юрисдикций

Данные в облаке могут передаваться между центрами обработки данных или даже через границы стран. В зависимости от страны размещения данные будут регулироваться различными применимыми юрисдикциями. Например, в некоторых юрисдикциях, например в Европейском союзе, требуется обеспечить всестороннюю защиту информации, позволяющей установить личность, которая, как правило, не может быть обработана в местах, не обеспечивающих достаточный уровень гарантированной защиты. Еще одним примером является возможное рассмотрение связи как услуги (CaaS) в некоторых юрисдикциях в качестве нерегулируемой информационной услуги, в то время как в других юрисдикциях она считается регулируемой услугой телефонной связи. Данный конфликт юрисдикций может привести к правовым осложнениям.

8.2.5 Риски, связанные с изменениями

Одно из преимуществ облачных вычислений заключается в возможности переноса некоторых решений с этапа разработки системы на этап реализации. Это значит, что некоторые зависящие от программного обеспечения компоненты системы могут быть отобраны и реализованы только тогда, когда выполнена функция, для которой требуются эти компоненты. Однако обычная методика оценки традиционных рисков более не подходит для такой динамично изменяющейся системы. В любой системе, прошедшей оценку безопасности на этапе разработки, могут возникнуть новые уязвимости, появившиеся в период ее эксплуатации в связи с изменениями программных компонентов.

8.2.6 Неудачный переход и интеграция

Переход в облако нередко подразумевает перенос больших объемов данных и серьезные изменения конфигурации (например, сетевую адресацию). Для перевода одной из частей системы ИКТ на обслуживание внешним CSP может потребоваться существенное измерение конструкции системы (например, сети и политики безопасности). Неудачная интеграция, вызванная несовместимыми интерфейсами или несогласованным выполнением политики, может привести как к функциональным, так и нефункциональным последствиям. Например, виртуальные машины, которые в частном центре обработки данных работают под защитой брандмауэра, в облаке CSP подвержены инцидентам открытого интернета.

8.2.7 Перебои в деятельности

При облачных вычислениях происходит распределение ресурсов и их предоставление как услуги. Вся экосистема облачных вычислений состоит из множества взаимозависимых частей. Перебои в работе любой части (например, отключение питания, отказ в обслуживании или задержка) могут затронуть готовность услуги облачных вычислений, рассматриваемую в пункте 8.1.5 "Неготовность услуги", и далее привести к перебоям в деятельности.

8.2.8 Привязка к партнеру облачной услуги

Платформа CSP создается с помощью программных и аппаратных компонентов различных поставщиков. Некоторые компоненты могут содержать проприетарные функции или расширения, которые необходимы для CSP. Однако использование этих проприетарных функций ограничивает возможность перехода CSP к другому поставщику компонентов.

Привязка является рабочей проблемой, при этом она, по сути, не является угрозой безопасности. Вместе с тем иногда она может вызывать обеспокоенность в отношении безопасности. Например, если CSN, который поставляет один из важнейших компонентов, прекращает свою деятельность, модули корректировки безопасности могут оказаться недоступными. В случае появления уязвимости в этом компоненте снижение риска может оказаться весьма сложным и дорогостоящим.

8.2.9 Уязвимость цепи поставок

CSP подвергается риску, если аппаратное или программное обеспечение, предоставляемое для платформы через его цепь поставок, подрывает безопасность CSC или CSP, например при случайном или намеренном внедрении вредоносного программного обеспечения или уязвимостей, которые могут эксплуатироваться.

В качестве примера можно привести дефектный код CSN. Данная проблема безопасности касается кода CSN, выполняемого на аппаратуре CSP, например клиентского программного обеспечения, виртуальной машины (VM), гостевой операционной системы (ОС), приложений, компонентов платформы или программного обеспечения для аудита/мониторинга (например, для партнера, обеспечивающего аудит услуги).

Еще одним примером является выполнение CSP кода, представляемого партнером; если партнер своевременно не предоставляет необходимые обновления безопасности, CSP подвергается риску.

8.2.10 Взаимозависимость программного обеспечения

При обнаружении уязвимости незамедлительное применение обновления может оказаться невозможным в связи с тем, что это приведет к нарушению работы других программных компонентов (несмотря на то что эти компоненты не требуют специального обновления). Это особенно справедливо в случае существования зависимости между компонентами, предоставленными одним или несколькими CSN, а не самими CSP.

8.3 Проблемы безопасности для партнеров облачной услуги (CSN)

В настоящем пункте рассматриваются проблемы, которые непосредственно затрагивают CSN. Такие проблемы могут затрагивать способность CSN осуществлять деятельность, получать оплату, защищать свою интеллектуальную собственность и избегать правовых или регуляторных трудностей. Проблемы безопасности, с которыми сталкивается тот или иной CSN, зависят от его конкретной деятельности и среды, например разработка, интеграция, аудит или другое.

8.3.1 Неопределенность в отношении ответственности

В случае если в услуге выполняется набор кодов CSP и CSN, для CSC может быть неочевидно, на ком лежит ответственность за ликвидацию последствий и обработку инцидентов безопасности. Может оказаться довольно трудно определить ответственную организацию с помощью технического анализа. В результате CSP и CSN будут перекладывать вину друг на друга, что может привести к дополнительным нарушениям, если не будет найдена основная причина.

8.3.2 Неправомерное присвоение интеллектуальной собственности

В случае если партнеры предоставляют CSP коды или другие ресурсы для выполнения, существует проблема безопасности, связанная с утечкой этих материалов, которые могут попасть к третьим сторонам, или их неправомерным присвоением с целью несанкционированного использования. Сюда входит нарушение авторского права или раскрытие коммерческой тайны.

8.3.3 Потеря целостности программного обеспечения

Поскольку программный код партнера выполняется CSP, существует возможность изменения кода или его заражения вирусом, когда он выходит из-под непосредственного контроля CSN. Таким образом, это приводит к неправильному функционированию программного обеспечения CSN, проявляющемуся тем или иным образом. Несмотря на то что CSN не в состоянии проконтролировать данную возможность, она может серьезно затронут его репутацию и, следовательно, его деятельность.

9 Возможности обеспечения безопасности облачных вычислений

В настоящей Рекомендации определяются следующие возможности обеспечения безопасности от выявленных угроз и проблем безопасности облачных вычислений. В соглашении об уровне обслуживания (SLA) могут быть указаны параметры, связанные с этими возможностями обеспечения безопасности, например время реагирования на инциденты.

9.1 Модель доверия

Для любой системы, в которой несколько поставщиков сотрудничают с целью оказания заслуживающей доверие услуги, необходима общая модель доверия.

В связи с чрезвычайно распределенным характером облачных вычислений, сопряженным с наличием нескольких участников, необходимо, чтобы среда облачных вычислений включала общую модель доверия. Эта модель доверия позволит создавать острова и/или федерации доверенных объектов, так чтобы разрозненные элементы системы могли аутентифицировать идентичность и санкционированные права других объектов и компонентов. Каждый остров федерации доверия будет основан на одном или нескольких доверенных органах выдачи сертификатов инфраструктуры открытых ключей (PKI).

Сегодня существует много моделей доверия, предназначенных для использования в облачной и необлачной среде. Вопрос о принятии конкретной модели доверия не входит в сферу применения настоящей Рекомендации.

9.2 Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций

К услугам облачных вычислений имеют отношение много администраторов и пользователей, при этом доступ к этим услугам и их использование осуществляются внутренним (CSP) и внешним (CSC) образом. Управление определением идентичности необходимо не только для защиты идентичностей, но и для упрощения процессов управления доступом, аутентификации, авторизации и аудита транзакций в такой динамичной и открытой инфраструктуре облачных вычислений.

Одна или несколько общих моделей безопасности (пункт 9.1) необходимы IAM для аутентификации идентичностей, а также разработчикам, гипервизорам и другим компонентам системы для аутентификации компонентов системы, например загруженных программных модулей, приложений и наборов данных.

Процесс IAM способствует обеспечению конфиденциальности, целостности и готовности услуг и ресурсов, и поэтому имеет важнейшее значение в облачных вычислениях.

Кроме того, IAM обеспечивает возможность осуществления однократной регистрации и реализации федерации идентичности в облаках с помощью различных механизмов аутентификации или механизмов, распределенных по различным доменам безопасности.

Аудит транзакций обеспечивает защиту от непризнания участия, позволяет осуществлять экспертно-технических анализ после инцидентов безопасности и является средством предотвращения атак (как внешних, так и внутренних вторжений). Аудит транзакций подразумевает не просто ведение журнала, а включает и активный мониторинг с целью привлечения внимания к подозрительным действиям.

9.3 Физическая безопасность

Необходимо, чтобы обеспечивалась физическая защита. Доступ в помещения, содержащие оборудование CSP, разрешается только авторизованным лицам и только в те области, которые непосредственно необходимы для выполнения их функциональных обязанностей; эта задача является частью процесса IAM. Однако степень физической безопасности зависит от ценности данных и масштабов доступа, разрешенного множеству пользователей.

9.4 Безопасность интерфейса

Данная возможность обеспечивает безопасность интерфейсов, открытых для CSC и/или других привлекаемых на основании договора CSP, с помощью которых доставляются различные виды услуг облачных вычислений, и обеспечивает безопасность взаимодействия, осуществляемого на основе этих интерфейсов. Доступные механизмы обеспечения безопасности включают, в том числе: одностороннюю/взаимную аутентификацию, контрольную сумму для проверки целостности, сквозное шифрование, цифровую подпись и т. д.

9.5 Безопасность виртуализации вычислений

Безопасность виртуализации вычислений относится к безопасности всей среды виртуализации вычислений. Эта возможность обеспечивает защиту гипервизора от атак, защиту хост-платформы от угроз, возникающих в среде виртуализации вычислений, и защиту виртуальных машин на протяжении их срока действия. В частности, данная возможность позволяет изолировать VM и защищать образы VM приостанавливать экземпляры VM при хранении и в процессе перехода.

Для CSP гипервизор нередко обеспечивает защиту размещенных VM путем предоставления антивирусной и антиспамовой обработки, осуществляемой внутри гипервизоров, с тем чтобы VM не требовалось отдельно реализовывать эти функции. Как привило, гипервизор оснащается минимальным набором услуг. Ненужные интерфейсы и интерфейсы прикладного программирования (API), как правило, закрываются, а неиспользуемые компоненты услуг, как правило, выключаются.

Виртуальные машины, на которые распространяется данная возможность, включают те машины, которые создаются CSC в IaaS, а также многие VM, создаваемые SaaS и PaaS. Виртуальные машины, как правило, надежно изолируются в случае совместного использования памяти, центрального процессора (ЦП) и емкости запоминающих устройств. Виртуальные машины, как правило, имеют собственные возможности обеспечения безопасности и информированы о политике (например, в гостевой операционной системе).

9.6 Безопасность сети

В среде облачных вычислений безопасность сети позволяет изолировать физическую и виртуальную сети и обеспечить безопасную связь между всеми участниками. Эта возможность делает доступным разбиение домена безопасности, средства управления доступа на границе сети (например, брандмауэр), обнаружение и предотвращение вторжения, разделение сетевого трафика на основе политики безопасности. Кроме того, она обеспечивает защиту сети от атак в средах физической и виртуальной сетей.

9.7 Изолирование и защита данных и защита конфиденциальности

С помощью данной возможности решаются общие проблемы защиты данных, которые нередко имеют правовые последствия.

- Изолирование данных

В контексте облачных вычислений, одна группа внутренних пользователей лишается возможности доступа к данным, принадлежащим другой группе внутренних пользователей, даже если эти данные зашифрованы, за исключением случаем, когда доступ санкционирован в явной форме. Изолирование данных может быть реализовано логически или физически, в зависимости от требуемого объема изолированных данных и конкретного развертывания программного и аппаратного обеспечения облачных вычислений.

ПРИМЕЧАНИЕ 1. – В среде облачных вычислений изолирование происходит на уровне группы внутренних пользователей. Тот или иной CSC может иметь несколько таких групп в облаке, например для разных филиалов, отделов или структурных подразделений.

- Защита данных

Защита данных обеспечивает надлежащую защиту данных CSC и производных данных, содержащихся в среде облачных вычислений, так чтобы доступ к ним и их изменение могли осуществляться только с санкции CSC (или в соответствии с применимым законодательством). Такая защита может включать некоторую комбинацию списков контроля доступа, проверку целостности, исправление ошибок/восстановление данных, шифрование и другие надлежащие механизмы.

В том случае, когда CSP обеспечивает для CSC шифрование данных на запоминающем устройстве, данная функция может быть шифрованием на стороне клиента (например, в приложении CSP) или шифрованием на стороне сервера.

- Защита конфиденциальности

Частная информация может включать PII и конфиденциальные корпоративные данные. Сбор, использование, передача, обработка, хранение и уничтожение частной информации регулируются нормативными или законодательными актами в отношении конфиденциальности. Данное ограничение применяется и к CSP, и к их CSC. Так, например, CSC должны иметь возможность постоянного удаления таблицы данных, содержащей частную информацию, даже если CSP не осведомлен о содержании таблицы. Кроме того, может потребоваться, чтобы CSP обеспечивал обработку, например поиск данных CSC в преобразованном или зашифрованном виде.

Защита конфиденциальности распространяется на частную информацию, которая может быть просмотрена или получена в результате деятельности CSC, например тенденции деловой активности, отношения или взаимодействие с другими сторонами, уровни и порядок действий и т. д.

Защита конфиденциальности отвечает и за обеспечение того, чтобы вся частная информация (включая наблюдаемые или производные данные) использовалась только в тех целях, которые были согласованы CSC и CSP.

Оценка риска в отношении частной информации, называемая "оценкой риска конфиденциальности", может помочь CSP в определении конкретных рисков нарушения конфиденциальности, связанных с предполагаемым функционированием. CSP следует определить и реализовать возможности для устранения рисков конфиденциальности, выявленных с помощью оценки риска и обработки частной информации.

ПРИМЕЧАНИЕ 2. – В некоторых юрисдикциях отдельные физические лица (например, пользователи-люди) рассматриваются отдельно от их работодателей для целей обеспечения конфиденциальности. В таких случаях обеспечивается надлежащая защита конфиденциальности пользователя облачной услуги (CSU), наряду с конфиденциальностью потребителя облачной услуги (CSC) или группы внутренних пользователей облачной услуги.

9.8 Координация обеспечения безопасности

В связи с тем, что в разных услугах облачных вычислений подразумеваются разные способы реализации средств управления безопасностью, с помощью данной возможности обеспечения безопасности координируются действия разнородных механизмов обеспечения безопасности, чтобы не допустить конфликтов механизмов защиты.

Стороны, выполняющие разные роли в экосистеме облачных вычислений, например CSP, CSC и CSN имеют разные степени контроля над физическими или виртуальными ресурсами и услугами, включая контроль безопасности.

Для каждой стороны существуют различные механизмы обеспечения безопасности, включающие изолирование гипервизора, IAM, защиту сети и т. д.

Одна из целей облачных вычислений заключается в обеспечении возможности объединения этих разных сторон в целях совместного проектирования, создания, развертывания и эксплуатации различных физических и виртуализованных ресурсов. В связи с этим необходимо, чтобы CSP имел возможность координировать разные механизмы обеспечения безопасности, используемые разными сторонами. Координация обеспечения безопасности зависит от функциональной совместимости и согласования разнообразных механизмов обеспечения безопасности.

9.9 Эксплуатационная безопасность

Данная возможность обеспечивает безопасность повседневной эксплуатации и технического обслуживания услуг и инфраструктуры облачных вычислений.

Данная возможность обеспечения эксплуатационной безопасности включает:

- определение набора принципов политики безопасности и деятельности по обеспечению безопасности, например управление конфигурацией, совершенствование корректировки, оценка безопасности, реагирование на инциденты (см. также пункт 9.10 "Управление инцидентами"), и обеспечение правильного применения этих мер безопасности в целях выполнения требований применимого законодательства и договоров, включая любые SLA, связанные с безопасностью.
- контроль выполнения CSP мер безопасности и их эффективности и предоставление надлежащих отчетов затронутым CSC, а также соответствующим сторонним аудиторам (действующим как CSN), позволяющим CSC оценить, обеспечивает ли CSP выполнение обязательств в области безопасности, предусмотренных SLA.

В случае изменения мер безопасности CSP и их эффективности все нижестоящие CSP и CSC оповещаются о таких изменениях.

Эти отчеты и оповещения позволяют авторизованным CSC просматривать информацию о соответствующих инцидентах, информацию аудита, а также данные конфигурации, относящиеся к их услугам облачных вычислений.

9.10 Управление инцидентами

Управление инцидентами предусматривает мониторинг и прогнозирование инцидентов, оповещение об инцидентах и реагирование на них. Для того чтобы знать, работает ли услуга облачных вычислений в штатном режиме в пределах всей инфраструктуры, необходим непрерывный мониторинг (например, мониторинг показателей работы виртуализированной платформы и виртуализированной машины в реальном времени). Это дает возможность системе собирать информацию о состоянии безопасности услуги, выявлять нештатные условия и обеспечивать раннее предупреждение о перегрузках системы безопасности, нарушениях работы, перебоях в обслуживании и т. д. После наступления событий инцидента безопасности обеспечивается выявление проблемы и быстрое реагирование на инцидент, осуществляемое либо автоматически, либо с вмешательством администратора-человека. Обработанные инциденты заносятся в журнал, и проводится их анализ с целью создания на их основе шаблонов, с помощью которых в дальнейшем обеспечивается упреждающая обработка.

9.11 Восстановительные работы при бедствиях

Восстановительные работы при бедствиях представляют собой возможность реагирования на критические бедствия в целях возможно скорейшего возвращения в безопасное состояние и возобновления штатной работы. Данная возможность обеспечивает непрерывность предоставления услуги при минимальном прерывании.

9.12 Оценка и аудит безопасности услуги

Данная возможность позволяет осуществлять оценку безопасности услуг облачных вычислений. Она позволяет авторизованной стороне производить проверку соответствия облачной услуги применимым требованиям обеспечения безопасности. Оценка безопасности или аудит безопасности могут осуществляться CSC, CSP или третьей стороной (CSN), а сертификация системы безопасности может выполняться авторизованной третьей стороной (CSN).

Для обеспечения взаимного понимания в отношении уровня безопасности между CSC и CSP вводятся надлежащие критерии безопасности.

Каждый CSP и каждая из его услуг может иметь уровень безопасности применительно к средствам управления безопасностью CSP и их эффективности. Объявленные уровни безопасности CSP и их услуг облегчают сравнение и выбор надлежащих CSP и услуг облачных вычислений. Для предоставления надежных, независимых и нейтральных оценок уровня безопасности могут использоваться независимые доверенные третьи стороны.

Во избежание проведения CSP отдельного аудита безопасности для каждого CSC надлежащим образом используются общие результаты аудита услуги. Для CSP, охватывающего широкий выбор услуг облачных вычислений, аудит безопасности может проводиться по каждой услуге облачных вычислений. CSP могут предоставлять авторизованному CSC (например, потенциальному потребителю), а также некоторым другим CSP и CSN (например, стороннему аудитору) надлежащие результаты аудита всех услуг облачных вычислений или части этих услуг.

Для цепи услуг облачных вычислений результаты аудита безопасности нижестоящего поставщика услуг включают соответствующие результаты аудита безопасности вышестоящего поставщика услуг.

9.13 Функциональная совместимость, переносимость и обратимость

Данная возможность разрешает сосуществование и взаимодействие разнородных компонентов (функциональная совместимость), разрешает CSC, при необходимости, заменять одного CSP другим (переносимость) и разрешает CSC перевод своей системы ИКТ из среды облачных вычислений обратно в инфраструктуру ИКТ на основе необлачных вычислений (обратимость). Обратимость также обеспечивает "право быть забытыми", если это требуется местными нормативными или законодательными актами.

ПРИМЕЧАНИЕ 1. – Данная возможность отвечает только за функциональную совместимость и переносимость функций безопасности облачных вычислений, а не фактических данных, метаданных или форматов сообщений, ответственность за которые лежит на других функциях платформы облачных вычислений. Например, данная возможность может обеспечивать шифрование при переходе, управление ключами и информацию об идентичности, так чтобы данные и другой контент можно было перенести между двумя разными системами шифрования, не открывая систему(ы) или данные при переходе.

ПРИМЕЧАНИЕ 2. – "Право быть забытыми" еще четко не определено и в некоторых случаях может ограничиваться регуляторными требованиями о сохранении в течение минимального периода времени определенных данных, например записей вызовов или информации о соединениях. В связи с этим может потребоваться сохранение в течение того же периода времени соответствующих ключей или другой информации, касающейся безопасности.

9.14 Безопасность цепи поставок

CSP использует ряд поставщиков для создания своих услуг. Некоторые из этих поставщиков являются участниками отрасли облачных вычислений, например CSN, в то время как другие поставщики являются традиционными поставщиками оборудования или услуг информационных технологий (ИТ), например производителями аппаратного обеспечения, не имеющими прямого отношения к облачным вычислениям. Данная возможность позволяет создавать отношения доверия между CSP и всеми участниками цепи поставок с помощью деятельности в области безопасности. Такая деятельность в области безопасности цепи поставок предусматривает определение и сбор информации о приобретенных CSP компонентах и услугах, которые используются для предоставления услуг облачных вычислений, и обеспечение соблюдения политики безопасности цепи поставок.

Например, типовая деятельность в области безопасности цепи поставок в CSP может включать:

- подтверждение справочной информации об участниках цепи поставок;
- валидацию аппаратного и программного обеспечения и услуг, применяемых CSP;
- проверку аппаратного и программного обеспечения, приобретаемого CSP с целью удостовериться в том, что оно не было подделано при транспортировке (передаче).
- предоставление механизмов проверки происхождения программного обеспечения для облачной услуги, например кода, предоставленного CSN. При необходимости, CSN и обеспечивающие их хостинг CSP обеспечивают процесс проверки целостности компонента программного обеспечения CSN, чтобы убедиться, что оно доставлено в надлежащем виде и не было изменено или взломано. Некоторые CSN могут потребовать предоставления средств для непосредственной самостоятельной проверки.

Данная возможность является непрерывной и охватывает постоянное развитие и обновление системы.

10 Базовая методика

Под разработкой основ безопасности облачных вычислений понимается получение представления о существующих угрозах и проблемах, рассмотренных в пунктах 7 и 8, для выбранной конкретной облачной услуги. Наряду с этим следует объединить деловые, технологические и регуляторные требования, для того чтобы определить средства управления, политику и процедуры безопасности, которые потребуются для той или иной облачной услуги. Описанные в пункте 9 возможности смягчения последствий угроз и решения проблем в дальнейшем используются для разработки средств управления, политики и процедур безопасности для выбранной конкретной услуги облачных вычислений. В настоящей Рекомендации основное внимание уделяется вопросу о том, какова необходимость обеспечения безопасности в среде облачных вычислений, и каковы угрозы и проблемы, характерные для среды традиционных вычислений, которые существуют в среде облачных вычислений. Соответственно, помимо настоящей Рекомендации, должны соблюдаться стандарты и примеры передового опыта, определенные отраслевыми организациями.

Методика, описанная в настоящей Рекомендации, должна соблюдаться при создании основ, определяющих средства управления, политику и процедуры безопасности, которые необходимы для какой-либо конкретной услуги облачных вычислений. Невозможно обеспечить единую нормативную основу для всех услуг облачных вычислений, так как они существенно различаются с точки зрения бизнес-моделей, предлагаемых услуг и вариантов реализации:

- Этап 1: Использовать пункты 7 и 8 для выявления угроз безопасности и последствий проблем для безопасности в рассматриваемой услуге облачных вычислений.
- Этап 2: Использовать пункт 9 для определения необходимых высокоуровневых возможностей обеспечения безопасности на основе выявленных угроз и проблем, которые могут уменьшить угрозы безопасности и решить проблемы безопасности.
- Этап 3: Получить средства управления, политику и процедуры безопасности, которые могут предоставить необходимые способности обеспечения безопасности исходя из определенных возможностей обеспечения безопасности.

ПРИМЕЧАНИЕ. – CSC и CSP необходимо определить набор надлежащих требований в отношении возможностей обеспечения безопасности, используя надлежащие стандарты. Данное определение основывается на оценке риска.

Для определения того, какие угрозы и проблемы безопасности соответствуют рассматриваемой облачной услуге, следует рассмотреть каждую угрозу или проблему. Один из простейших возможных методов заключается в составлении таблицы с указанием символа "Y" напротив угрозы или проблемы.

В качестве примера использования данного метода рассмотрим случай, когда CSP предлагает индивидуальным пользователям хранение файлов как услугу. CSP хотел бы знать, какие угрозы и проблемы безопасности вызывают наибольшую обеспокоенность пользователей, и проанализировать вопрос о том, какие угрозы и проблемы ему необходимо устранить в первую очередь. Данный метод наглядно иллюстрируется в таблице 1.

Таблица 1 – Пример проведения этапа 1 анализа, предусмотренного основами безопасности, для случая хранения файлов как услуги

Область проведения анализа	Конкретная угроза или проблема	Применимо ли к данной услуге?
Пункт 7.1 Угрозы безопасности для потребителей облачной услуги (CSC)	Пункт 7.1.1 Потеря и утечка данных	Y
	Пункт 7.1.2 Незащищенный доступ к услуге	Y
	Пункт 7.1.3 Внутренние угрозы	
Пункт 7.2 Угрозы безопасности для поставщиков облачной услуги (CSP)	Пункт 7.2.1 Несанкционированный административный доступ	Y
	Пункт 7.2.2 Внутренние угрозы	Y
Пункт 8.1 Проблемы безопасности для потребителей облачной услуги (CSC)	Пункт 8.1.1 Неопределенность в отношении ответственности	Y
	Пункт 8.1.2 Потеря доверия	Y
	Пункт 8.1.3 Потеря управления	Y
	Пункт 8.1.4 Потеря конфиденциальности	Y
	Пункт 8.1.5 Неготовность услуги	Y
	Пункт 8.1.6 Привязка к одному поставщику облачной услуги	Y
	Пункт 8.1.7 Неправомерное присвоение интеллектуальной собственности	
	Пункт 8.1.8 Потеря целостности программного обеспечения	
Пункт 8.2 Проблемы безопасности для поставщиков облачной услуги (CSP)	Пункт 8.2.1 Неопределенность в отношении ответственности	Y
	Пункт 8.2.2 Совместно используемая среда	Y
	Пункт 8.2.3 Несогласованность и конфликт механизмов защиты	Y
	Пункт 8.2.4 Конфликт юрисдикций	Y
	Пункт 8.2.5 Риски, связанные с изменениями	
	Пункт 8.2.6 Неудачный переход и интеграция	Y
	Пункт 8.2.7 Перебои в деятельности	Y
	Пункт 8.2.8 Привязка к партнеру облачной услуги	
	Пункт 8.2.9 Уязвимость цепи поставок	Y
	Пункт 8.2.10 Взаимозависимость программного обеспечения	
Пункт 8.3 Проблемы безопасности для партнеров облачной услуги (CSN)	Пункт 8.3.1 Неопределенность в отношении ответственности	
	Пункт 8.3.2 Неправомерное присвоение интеллектуальной собственности	
	Пункт 8.3.3 Потеря целостности программного обеспечения	

После выявления угроз и проблем безопасности можно определить возможности обеспечения безопасности, которые могли бы смягчить последствия этих угроз и решить эти проблемы. В таблице I.1 приведен пример преобразования угроз и проблем безопасности облачных вычислений в возможности обеспечения безопасности. Символ "Y" в ячейке, образованной пересечением столбцов и строк таблицы, обозначает, что та или иная конкретная угроза и проблема безопасности устраняется с помощью соответствующей возможности обеспечения безопасности. В этой таблице показаны все угрозы и проблемы и соответствующие им возможности обеспечения безопасности.

После определения требуемых возможностей можно определить необходимые средства управления, политику и процедуры безопасности. Примеры средств управления, которые могут быть использованы, включают "Безопасность операций" (пункт 12 в [b-ISO/IEC 27002]) и "Управление инцидентами информационной безопасности" (пункт 16 в [b-ISO/IEC 27002]). Они могут быть получены из возможностей, определенных в пунктах 9.9 и 9.10, соответственно.

Облачная услуга может иметь цепь поставок, состоящую из нескольких CSP. Компании, участвующие в такой цепи поставок, могут обращаться к стандартам МСЭ и отраслевым стандартам на тему безопасности цепи поставок (например, [b-ISO/IEC 28000]). Необходимо, чтобы каждый CSP четко разграничил свою ответственность в цепи услуги облачных вычислений и разработал свои средства управления, политику и процедуры безопасности, которые основаны на возможностях обеспечения безопасности, полученных в результате этого трехэтапного метода. Для обеспечения согласованной безопасности CSC вышестоящему CSP, возможно, потребуется договориться со своими нижестоящими CSP относительно этих возможностей обеспечения безопасности, исходя из своих сфер ответственности в области безопасности. При необходимости CSC также должны следовать этой трехэтапной процедуре.

Кроме того, указанную выше трехэтапную процедуру следует осуществлять через определенные промежутки времени или при необходимости (например, при наступлении случаев серьезного нарушения безопасности или при изменении CSP своего вышестоящего CSP).

Дополнение I

Соответствие угроз и проблем безопасности облачных вычислений возможностям обеспечения безопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В таблице I.1 показано соответствие угроз и проблем безопасности облачных вычислений некоторым допустимым возможности обеспечения безопасности.

Символ "Y" в ячейке, образованной пересечением столбцов и строк таблицы, обозначает, что та или иная конкретная угроза и проблема безопасности устраняется с помощью соответствующей возможности обеспечения безопасности.

Таблица I.1 – Соответствие угроз и проблем безопасности облачных вычислений возможностям обеспечения безопасности

			Пункт 9 Возможности обеспечения безопасности облачных вычислений													
			Пункт 9.1 Модель доверия	**Пункт 9.2 Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций**	**Пункт 9.3 Физическая безопасность**	**Пункт 9.4 Безопасность интерфейса**	**Пункт 9.5 Безопасность виртуализации вычислений**	**Пункт 9.6 Безопасность сети**	**Пункт 9.7 Изолирование и защита данных и защита конфиденциальности**	**Пункт 9.8 Координация обеспечения безопасности**	**Пункт 9.9 Эксплуатационная безопасность**	**Пункт 9.10 Управление инцидентами**	**Пункт 9.11 Восстановительные работы при бедствиях**	**Пункт 9.12 Оценка и аудит безопасности услуги**	**Пункт 9.13 Функциональная совместимость, переносимость и обратимость**	**Пункт 9.14 Безопасность цепи поставок**
Пункт 7 Угрозы безопасности облачных вычислений	Пункт 7.1 Угрозы безопасности для потребителей облачной услуги (CSC)	Пункт 7.1.1 Потеря и утечка данных	Y	Y	Y				Y				Y			
		Пункт 7.1.2 Незащищенный доступ к услуге	Y	Y		Y	Y	Y								
		Пункт 7.1.3 Внутренние угрозы		Y	Y									Y		
	Пункт 7.2 Угрозы безопасности для поставщиков облачной услуги (CSP)	Пункт 7.2.1 Несанкционированный административный доступ	Y	Y	Y	Y										
		Пункт 7.2.2 Внутренние угрозы		Y	Y									Y		

Таблица I.1 – Соответствие угроз и проблем безопасности облачных вычислений возможностям обеспечения безопасности

			Пункт 9 Возможности обеспечения безопасности облачных вычислений														
			Пункт 9.1 Модель доверия	**Пункт 9.2 Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций**	**Пункт 9.3 Физическая безопасность**	**Пункт 9.4 Безопасность интерфейса**	**Пункт 9.5 Безопасность виртуализации вычислений**	**Пункт 9.6 Безопасность сети**	**Пункт 9.7 Изолирование и защита данных и защита конфиденциальности**	**Пункт 9.8 Координация обеспечения безопасности**	**Пункт 9.9 Эксплуатационная безопасность**	**Пункт 9.10 Управление инцидентами**	**Пункт 9.11 Восстановительные работы при бедствиях**	**Пункт 9.12 Оценка и аудит безопасности услуги**	**Пункт 9.13 Функциональная совместимость, переносимость и обратимость**	**Пункт 9.14 Безопасность цепи поставок**
Пункт 8 Проблемы безопасности облачных вычислений	Пункт 8.1 Проблемы безопасности для потребителей облачной услуги (CSC)	Пункт 8.1.1 Неопределенность в отношении ответственности		Y							Y					
		Пункт 8.1.2 Потеря доверия	Y											Y		
		Пункт 8.1.3 Потеря управления		Y	Y				Y		Y	Y	Y	Y		
		Пункт 8.1.4 Потеря конфиденциальности		Y					Y					Y		
		Пункт 8.1.5 Неготовность услуги								Y	Y	Y	Y			Y
		Пункт 8.1.6 Привязка к одному поставщику облачной услуги													Y	
		Пункт 8.1.7 Неправомерное присвоение интеллектуальной собственности		Y	Y				Y		Y					
		Пункт 8.1.8 Потеря целостности программного обеспечения		Y			Y		Y							

Таблица I.1 – Соответствие угроз и проблем безопасности облачных вычислений возможностям обеспечения безопасности

			Пункт 9 Возможности обеспечения безопасности облачных вычислений														
			Пункт 9.1 Модель доверия	**Пункт 9.2 Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций**	**Пункт 9.3 Физическая безопасность**	**Пункт 9.4 Безопасность интерфейса**	**Пункт 9.5 Безопасность виртуализации вычислений**	**Пункт 9.6 Безопасность сети**	**Пункт 9.7 Изолирование и защита данных и защита конфиденциальности**	**Пункт 9.8 Координация обеспечения безопасности**	**Пункт 9.9 Эксплуатационная безопасность**	**Пункт 9.10 Управление инцидентами**	**Пункт 9.11 Восстановительные работы при бедствиях**	**Пункт 9.12 Оценка и аудит безопасности услуги**	**Пункт 9.13 Функциональная совместимость, переносимость и обратимость**	**Пункт 9.14 Безопасность цепи поставок**
Пункт 8 Проблемы безопасности облачных вычислений	Пункт 8.2 Проблемы безопасности для поставщиков облачной услуги (CSP)	Пункт 8.2.1 Неопределенность в отношении ответственности		Y							Y					
		Пункт 8.2.2 Совместно используемая среда					Y	Y	Y							
		Пункт 8.2.3 Несогласованность и конфликт механизмов защиты								Y					Y	
		Пункт 8.2.4 Конфликт юрисдикций							Y		Y					
		Пункт 8.2.5 Риски, связанные с изменениями									Y				Y	Y
		Пункт 8.2.6 Неудачный переход и интеграция				Y	Y	Y	Y	Y	Y					
		Пункт 8.2.7 Перебои в деятельности										Y	Y			
		Пункт 8.2.8 Привязка к партнеру облачной услуги														Y
		Пункт 8.2.9 Уязвимость цепи поставок														Y
		Пункт 8.2.10 Взаимозависимость программного обеспечения														Y

Таблица I.1 – Соответствие угроз и проблем безопасности облачных вычислений возможностям обеспечения безопасности

			Пункт 9 Возможности обеспечения безопасности облачных вычислений														
			Пункт 9.1 Модель доверия	**Пункт 9.2 Управление определением идентичности и доступом (IAM), аутентификация, авторизация и аудит транзакций**	**Пункт 9.3 Физическая безопасность**	**Пункт 9.4 Безопасность интерфейса**	**Пункт 9.5 Безопасность виртуализации вычислений**	**Пункт 9.6 Безопасность сети**	**Пункт 9.7 Изолирование и защита данных и защита конфиденциальности**	**Пункт 9.8 Координация обеспечения безопасности**	**Пункт 9.9 Эксплуатационная безопасность**	**Пункт 9.10 Управление инцидентами**	**Пункт 9.11 Восстановительные работы при бедствиях**	**Пункт 9.12 Оценка и аудит безопасности услуги**	**Пункт 9.13 Функциональная совместимость, переносимость и обратимость**	**Пункт 9.14 Безопасность цепи поставок**
Пункт 8 Проблемы безопасности облачных вычислений	Пункт 8.3 Проблемы безопасности для партнеров облачной услуги (CSN)	Пункт 8.3.1 Неопределенность в отношении ответственности		Y							Y						
		Пункт 8.3.2 Неправомерное присвоение интеллектуальной собственности		Y	Y				Y		Y						
		Пункт 8.3.3 Потеря целостности программного обеспечения		Y			Y		Y								

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.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ISO/IEC 19440] ISO/IEC 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

[b-ISO/IEC 28000] ISO/IEC 28000:2007, *Specification for security management systems for the supply chain*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.

[b-CSA Matrix] CSA (2013), *Cloud Controls Matrix,* Cloud Security Alliance.

[b-key definition] Key definitions of the Data Protection Act, Information Commissioners Office <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
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 и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2014 г.