Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1642

(03/2016)

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

Безопасность облачных вычислений – Передовой опыт и руководящие указания в области облачных вычислений

Руководящие указания по эксплуатационной безопасности облачных вычислений

Рекомендация МСЭ-Т X.1642

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
Рекомендации, связанные с PKI	X.1340–X.1349
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.1642

Руководящие указания по эксплуатационной безопасности облачных вычислений

Резюме

В Рекомендации МСЭ-Т X.1642 представлены общие руководящие указания по эксплуатационной безопасности облачных вычислений с точки зрения поставщиков облачных услуг (CSP). В ней анализируются требования к безопасности и показатели безопасности для операций по облачным вычислениям. Представлен комплекс мер по обеспечению безопасности и подробно описана деятельность в области безопасности в рамках повседневной эксплуатации и техническом обслуживании, с тем чтобы помочь CSP в смягчении рисков для безопасности и решения связанных с безопасностью проблем для операций по облачным вычислениям.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1642	23.03.2016 г.	17-я	11.1002/1000/12616

Ключевые слова

Облачные вычисления, эксплуатационная безопасность, пункт о безопасности в соглашении об уровне обслуживания (SLA).

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

ПРЕДИСЛОВИЕ

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

Рекомендация МСЭ-Т X.1642

Руководящие указания по эксплуатационной безопасности облачных вычислений

1 Сфера применения

В настоящей Рекомендации проясняются взаимные обязанности поставщиков облачных услуг (CSP) и потребителей облачных услуг (CSC) в области безопасности, а также анализируются требования к безопасности и категории показателей эксплуатационной безопасности облачных вычислений. Дается подробное описание направленных на выполнение требований к эксплуатационной безопасности облачных вычислений комплексов мер, и деятельности по обеспечению безопасности в рамках повседневной эксплуатации и технического обслуживания служб и инфраструктуры облачных вычислений с точки зрения CSP.

Данная Рекомендация поможет CSP в снижении уровня эксплуатационных рисков. Целевая аудитория настоящей Рекомендации – поставщики облачных услуг, такие как традиционные операторы электросвязи и поставщики услуг интернета (ПУИ).

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 облачные вычисления (cloud computing) [b-ITU-T Y.3500]: 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.

3.1.2 облачная услуга (cloud service) [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, обращение к которым производится с помощью заявленного интерфейса.

3.1.3 потребитель облачной услуги (cloud service customer) [b-ITU-T Y.3500]: Сторона, которая состоит в коммерческих отношениях применительно к использованию облачных услуг.

3.1.4 партнер по облачной услуге (cloud service partner) [b-ITU-T Y.3500]: Сторона, участвующая в поддержке деятельности поставщика или потребителя облачной услуги или того и другого либо оказывающая помощь в этой деятельности.

3.1.5 поставщик облачной услуги (cloud service provider) [b-ITU-T Y.3500]: Сторона, которая предоставляет облачные услуги.

3.1.6 инфраструктура как услуга (infrastructure as a service (IaaS)) [b-ITU-T Y.3500]: Категория облачных услуг, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, являются возможности инфраструктуры.

3.1.7 множественная принадлежность (multi-tenancy) [b-ITU-T Y.3500]: Распределение физических или виртуальных ресурсов, при котором несколько групп внутренних пользователей и их вычисления и данные изолированы друг от друга и недоступны друг другу.

3.1.8 сеть как услуга (network as a service (NaaS)) [b-ITU-T Y.3500]: Категория облачных услуг, в которой потребителю облачной услуги предоставляются возможности транспортного соединения и связанные с этим сетевые возможности.

3.1.9 сторона (party) [b-ISO 27729]: Физическое лицо, организация либо группа тех или других.

3.1.10 платформа как услуга (platform as a service (PaaS)) [b-ITU-T Y.3500]: Категория облачных услуг, в которой типом облачных возможностей, предоставляемых потребителю услуги, являются возможности платформы.

3.1.11 проблема безопасности (security challenge) [b-ITU-T X.1601]: Отличная от непосредственной угрозы безопасности "трудность", включающая "косвенные" угрозы, которая обусловлена характером и рабочей средой облачных услуг.

3.1.12 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.

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

3.1.14 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.

3.1.15 программное обеспечение как услуга (software as a service (SaaS)) [b-ITU-T Y.3500]: Категория облачных услуг, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, являются возможности приложения.

3.1.16 группа внутренних пользователей (tenant) [b-ITU-T Y.3500]: Один или несколько пользователей облачной услуги, совместно использующих доступ к набору физических и виртуальных ресурсов.

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

3.1.18 уязвимость (vulnerability) [b-NIST-SP-800-30]: Слабое место информационной системы, процедур обеспечения безопасности системы, внутренних средств управления или реализации, на которое может быть направлено действие источника угрозы.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ACL	Access Control List	Список управления доступом
API	Application Programming Interface	Интерфейс прикладного программирования
BIA	Business Impact Analysis	Анализ последствий для деятельности
CCTV	Closed Circuit Television	Система видеонаблюдения
CPU	Central Processing Unit	Центральный процессор
CSC	Cloud Service Customer	Потребитель облачной услуги
CSN	Cloud Service Partner	Партнер по облачной услуге
CSP	Cloud Service Provider	Поставщик облачной услуги
DB	Database	База данных
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DLP	Data Leakage Prevention	Предотвращение утечки данных

DoS	Denial of Service		Отказ в обслуживании
IAM	Identity and Access Management		Управление определением идентичности и доступом
IaaS	Infrastructure as a Service		Инфраструктура как услуга
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
IdM	Identity Management		Управление определением идентичности
IDS	Intrusion Detection System		Система обнаружения проникновений
IP	Internet Protocol		Интернет-протокол
IPS	Intrusion Prevention System		Система предотвращения проникновений
ISP	Internet Service Provider	ПУИ	Поставщик услуг интернета
IT	Information Technology		Информационные технологии
JIT access	Just In Time access		Своевременный доступ
LDAP	Lightweight Directory Access Protocol		Облегченный протокол доступа к сетевому каталогу
NaaS	Network as a Service		Сеть как услуга
OS	Operating System	ОС	Операционная система
PaaS	Platform as a Service		Платформа как услуга
RPO	Recovery Point Objective		Целевая точка восстановления
RTO	Recovery Time Objectives		Целевые сроки восстановления
SaaS	Software as a Service		Программное обеспечение как услуга
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SMS	Short Message Service		Служба коротких сообщений
SSO	Single Sign-On		Однократная регистрация входа
VDC	Virtual Data Centre		Виртуальный центр обработки данных
VM	Virtual Machine		Виртуальная машина

5 Условные обозначения

Отсутствуют.

6 Общие сведения

В условиях стремительного расширения рынка облачных вычислений и образования соответствующих отраслевых цепочек проблемы безопасности остаются основной и важной темой, которую нельзя обходить вниманием. С облачными вычислительными системами связано бóльшее количество трудностей, чем с традиционными информационно-технологическими системами (ИТ-системами), так как они сложнее и в них хранятся огромные объемы принадлежащих пользователям конфиденциальных данных. Обеспечение безопасности и защита конфиденциальности – наиважнейшие факторы при оценке потребителями использования услуг облачных вычислений.

В перспективе предложение облачных услуг будет расширяться, и потребность в методах обеспечения их надежности становится все насущнее. В связи с этим необходимо всесторонне оценить эксплуатационную безопасность облачных вычислений в целях разработки руководящих указаний для поставщиков облачных услуг (CSP). Пользуясь этими руководящими указаниями, CSP смогут снизить риск, связанный с ненадлежащей эксплуатацией, неразумной организацией деятельности и т. п., а также повысить общий уровень эксплуатационной безопасности облачных вычислительных систем.

С точки зрения CSP обеспечение эксплуатационной безопасности сопряжено со следующими основными проблемами.

1) Проблемы технического обслуживания инфраструктуры облачных вычислений. Когда пользователям облачной системы предоставляются в качестве услуг ИТ-инфраструктура, платформа или программное обеспечение, необходимым условием ведения деятельности является стабильность, надежность и безопасность предоставления этих услуг. В целях обеспечения бесперебойного оказания услуги потребителям необходимо наладить надежную и устойчивую работу инфраструктуры облачной системы, а также принять необходимые меры для безопасности и защиты конфиденциальности принадлежащей пользователям информации. Даже при небольшом по масштабам отказе многие потребители облачных услуг (CSC) могут столкнуться с трудностями в виде перебоя в работе или потери данных. Поставщикам облачных услуг следует серьезно рассмотреть способы локализации сбоев и беспрепятственного автоматического переключения на резервную систему в целях обеспечения бесперебойной доступности услуги для потребителей.
2) Проблемы режима управления облачными вычислениями. От традиционных ИТ-услуг облачные вычисления отличаются такими характеристиками, как межрегиональные масштабы обслуживания, громадная вычислительная мощность и разделение между управлением и владением данными. В связи с этим для решения проблем безопасности поставщикам облачных услуг необходимо обеспечить эффективное управление и взаимодействие между филиальными узлами. Некоторым из поставщиков облачных услуг потребуется принять ряд технических мер, в частности по управлению конфигурацией системы безопасности, рациональному распределению управленческих полномочий и выработке действенных регламентов и процессов для предотвращения утечки пользовательских данных. Например, поставщикам облачных услуг следует принять меры к предотвращению превышения полномочий внутренними администраторами во избежание злоупотреблений облачными вычислительными ресурсами со стороны пользователей.

Для комплексного обеспечения безопасности облачных приложений, работающих на базе облачной инфраструктуры, поставщикам облачных услуг следует применять различные технические методы и механизмы управления, которые обеспечили бы не только устойчивость и доступность облачной инфраструктуры, но также и непрерывность ведения деятельности и защиту пользовательских данных в эксплуатируемых облачных системах.

7 Требования пункта о безопасности в соглашении об уровне обслуживания (SLA)

Пункт о безопасности в соглашении об уровне обслуживания (SLA) – важнейший фактор, обусловливающий доверие пользователей к поставщику облачных услуг. В этом пункте следует четко определить взаимоотношения между поставщиками и потребителями облачных услуг, в частности распределение между ними обязанностей по обеспечению безопасности. Поставщикам облачных услуг следует сосредоточить свои меры эксплуатационной безопасности на выполнении требований пункта о безопасности в соглашении об уровне обслуживания.

7.1 Распределение обязанностей по обеспечению безопасности между поставщиками и потребителями облачных услуг

Обязанности поставщиков и потребителей облачных услуг по обеспечению безопасности облачных вычислений следует четко разграничить в соответствии со степенью и характером их контроля над облачными вычислительными ресурсами и инфраструктурой.

Обязанности по обеспечению безопасности тесно связаны с режимом предоставления облачной услуги, так как последний отражает степень и характер контроля поставщиков и потребителей облачных услуг над ресурсами облачной среды. Например, поставщикам облачных услуг, предоставляющим программное обеспечение как услугу (SaaS) в отличие от услуг платформы (PaaS) или инфраструктуры (IaaS), следует брать на себя больший объем обязанностей в сфере безопасности, так как они в большей степени контролируют ресурсы.

В режиме инфраструктуры как услуги (IaaS) поставщики облачных услуг предоставляют инфраструктуру, например виртуальный центр обработки данных (VDC) с размещенными в нем серверами, хранилищем данных, сетью и средствами управления. К основным обязанностям поставщиков облачных услуг в этом случае относится обеспечение физической безопасности, безопасности сети, безопасности основополагающих систем и всей облачной инфраструктуры. К ведению потребителей облачных услуг следует отнести все вопросы безопасности выше уровня приобретаемой облачной инфраструктуры, например безопасность гостевой операционной системы (ОС), прикладного программного обеспечения и т. д.

В режиме платформы как услуги (PaaS) поставщики облачных услуг предоставляют упрощенную распределенную среду для разработки, тестирования и развертывания программного обеспечения. В круг обязанностей поставщиков облачных услуг в этом случае следует включить обеспечение безопасности интерфейса прикладного программирования (API) среды приложений, безопасности промежуточных программных средств, доступности облачной платформы и т. д., а также безопасности основополагающей инфраструктуры. В этом случае потребителям облачных услуг следует взять на себя ответственность за безопасность прикладных услуг, предоставляемых выше среды облачной платформы.

В режиме программного обеспечения как услуги (SaaS) поставщикам облачных услуг следует обеспечивать общую безопасность от инфраструктурного до прикладного уровня, а потребителям облачных услуг – информационную безопасность в зоне своего контроля, например безопасное управление определением идентичности (IdM), защиту от утечки паролей и т. д.

Кроме того, потребителям облачных услуг следует учитывать вопросы безопасности терминалов, которые они используют для доступа в облако.

7.2 Требования пункта о безопасности в соглашении об уровне обслуживания (SLA)

7.2.1 Общие требования

В пункте соглашения об уровне обслуживания (SLA), регулирующем вопросы безопасности, следует отчетливо изложить условия обеспечения безопасности облачных услуг, а также определить круг обязанностей и ответственность поставщиков и потребителей облачных услуг.

Для потребителей облачных услуг следует предусмотреть возможность изложить свои требования к указанному пункту SLA. Пункт о безопасности поможет им заручиться гарантией того, что поставщик услуги обеспечил достаточную защиту их информационных активов, ресурсов и индивидуально адаптированных услуг в процессе хранения, использования и передачи, а также реализовал механизмы выполнения нормативных требований к защите конфиденциальности данных в действующей юрисдикции.

Применительно к поставщикам облачных услуг пункт SLA о безопасности предусматривает требования к безопасности предоставляемых облачных услуг и соответствующие измеримые показатели, которые могут оцениваться, сравниваться и индивидуально адаптироваться потребителями облачных услуг. Поставщикам облачных услуг следует реализовать ряд надлежащих технических и управленческих механизмов для повышения надежности и безопасности облачных услуг, а также для выполнения требований пункта SLA о безопасности, что в конечном счете и обеспечит им доверие со стороны потребителей облачных услуг. К облачным службам могут применяться различные типы SLA в зависимости от содержания услуг, их класса и даже региона, в котором они предоставляются, но как минимум содержание пункта SLA о безопасности должно соответствовать нормативно-законодательным требованиям, а также требованиям соответствующих открытых отраслевых стандартов.

Конкретные требования пункта SLA о безопасности могут устанавливаться по соглашению между поставщиком и потребителем облачных услуг исходя из индивидуально адаптированных требований последнего, а также характера и степени его контроля над ресурсами. Во избежание лишних споров или рисков нарушения безопасности следует четко сформулировать положения об ограничении ответственности поставщика облачных услуг в контракте или описании продукта, с тем чтобы поставщик не нес ответственности в случае наступления обстоятельств непреодолимой силы.

7.2.2 Составные элементы пункта о безопасности в соглашении об уровне обслуживания (SLA)

Пункт о безопасности в соглашении об уровне обслуживания (SLA) включает в себя, помимо прочего, следующие элементы.

7.2.2.1 Обеспечение непрерывности деятельности

Поставщикам облачных услуг следует предусмотреть надлежащую защиту на случай антропогенных катастроф или стихийных бедствий в целях обеспечения доступности услуг и непрерывности деятельности. Конкретные требования изложены ниже.

1) Доступность услуги

   Процентная доля заданного промежутка времени, в течение которой услуга доступна для использования. В общем случае условия предоставления конкретной облачной услуги не должны предусматривать более низкую доступность, чем у традиционной информационно-коммуникационной услуги.

2) Среднее время восстановления

   Время, требуемое для восстановления потерянных данных или возобновления предоставления услуги после сбоя или чрезвычайной ситуации.

7.2.2.2 Защита данных

Поставщикам облачных услуг следует предусмотреть всеобъемлющую программу защиты данных, принадлежащих потребителям облачных услуг, и другой конфиденциальной информации, а также в деталях договориться с потребителями облачных услуг о соответствующих механизмах и требованиях.

1) Физическая безопасность хранилищ данных

   Поставщикам облачных услуг следует принять меры к обеспечению физической безопасности хранилищ данных посредством пропускного режима, системы противопожарной защиты, системы резервного электропитания и т. д.

2) Защита носителей данных

   Поставщикам облачных услуг следует принять меры к повышению защищенности носителей данных, такие как усиление защиты устройств, внесение исправлений и т. д.

3) Шифрование данных

   Следует указать, какие данные шифруются в процессе хранения или передачи, и привести подробные сведения об алгоритмах шифрования.

4) Контроль доступа к данным

   Следует предусмотреть меры по контролю доступа к данным, позволяющие предотвратить несанкционированный доступ.

5) Изоляция данных

   Следует предусмотреть логическую или физическую изоляцию данных, принадлежащих разным потребителям облачных услуг.

6) Удаление данных

   Следует предусмотреть гарантированное удаление данных перед выделением тех же ресурсов другим потребителям облачных услуг.

7) Резервное копирование данных

Следует определить целевую точку восстановления (RPO), целевые сроки восстановления (RTO), политику хранения данных, параметры комплексного локального и удаленного резервного копирования и т. д.

8) Аудит работы с данными

Поставщикам облачных услуг следует организовывать аудит работы с данными потребителей облачных услуг с возможностью выявления аномалий. Аудитор должен иметь сертификат, подтверждающий его квалификацию.

9) Соблюдение нормативно-законодательных требований к работе с данными

Сбор, передача, обработка, хранение и уничтожение данных должны производиться в соответствии с нормативно-законодательными требованиями, действующими в юрисдикции потребителя облачных услуг. Аналогичным образом требования к хранению данных должны соответствовать ограничениям, действующим в различных юрисдикциях.

7.2.2.3 Меры реагирования в чрезвычайных ситуациях

Поставщикам облачных услуг следует организовать телефонную горячую линию для оповещения о сбоях, функционирующую по будням в рабочее время или круглосуточно. В число показателей качества обслуживания следует включить срок подтверждения сбоя, срок диагностирования и устранения неисправности и тому подобные параметры.

7.2.2.4 Меры безопасности

Поставщикам облачных услуг следует принять надлежащие меры безопасности в отношении всей инфраструктуры облачных вычислений.

1) Меры по виртуализации вычислений

Поставщикам облачных услуг следует принять доступные меры к реализации анализа потока данных, виртуального брандмауэра или других функций безопасности на уровне гипервизора для обеспечения прозрачности и подконтрольности администраторам происходящего внутри виртуальных машин (VM).

2) Изоляция сетей и доменов

Поставщикам облачных услуг следует принять меры к изоляции сетей и доменов посредством брандмауэров, списков контроля доступа (ACL) в маршрутизаторах, а также контроллеров доменов и т. д. для обеспечения строгой изоляции различных потребителей облачных услуг друг от друга.

3) Привилегированный доступ

Поставщикам облачных услуг следует принять меры к обеспечению привилегированного доступа, например путем реализации своевременного (JIT) доступа.

4) Аутентификация

Поставщикам облачных услуг следует реализовать надежные методы аутентификации, такие как многофакторная аутентификация, аутентификация по отпечаткам пальцев и т. д., для повышения безопасности аутентификации.

5) Меры по обеспечению безопасности сетевого трафика

Поставщикам облачных услуг следует принять доступные меры к отражению атак типа "отказ в обслуживании" (DoS) и "распределенный отказ в обслуживании" (DDoS), обходу перегруженных участков сетей, а также развертыванию средств обнаружения или предотвращения проникновений в сеть.

6) Меры по защите от вредоносного программного обеспечения

Поставщикам облачных услуг следует принять доступные меры к предотвращению заражения вредоносным программным обеспечением и вирусами.

7) Внесение исправлений

Поставщикам облачных услуг следует обеспечить регулярное внесение исправлений и обновлений программного обеспечения для виртуализации, операционной системы и базы данных в целях поддержания этих программных средств в актуальном состоянии.

7.2.2.5 Аудит безопасности

Поставщикам облачных услуг следует организовывать регулярные аудиты всей облачной вычислительной системы. Такие мероприятия могут проводиться силами независимой внутренней аудиторской группы или сторонних аудиторов, действующих в качестве партнеров по облачной услуге (CSN). Результаты аудита следует надлежащим образом доводить до сведения потребителей облачных услуг.

7.2.2.6 Мониторинг безопасности в целях совершенствования соглашения об уровне обслуживания (SLA)

Поставщикам облачных услуг следует предусмотреть механизм мониторинга количественных показателей в целях совершенствования соглашения об уровне обслуживания.

1) Объекты мониторинга

Следует определить объекты мониторинга, такие как использование центрального процессора (CPU), предупреждения системы безопасности и т. д. Следует также явным образом определить сигнальные условия.

2) Уведомления о событиях, связанных с безопасностью

Следует указать способ и срок уведомления о событиях, связанных с безопасностью. Способом уведомления могут служить электронная почта, телефон, короткие сообщения или что-либо другое по договоренности между поставщиками и потребителями облачных услуг. Под сроком уведомления понимается среднее время, проходящее с наступления события до уведомления потребителя облачной услуги.

Поставщики облачных услуг могут предоставлять потребителям облачных услуг соответствующие возможности, например средства для самостоятельного мониторинга уровня обслуживания и автоматического контроля выделенных им ресурсов.

7.2.2.7 Сертификация в области безопасности

Обязанности по получению соответствующих сертификатов в области безопасности следует возложить на поставщиков облачных услуг. Им также следует регулярно продлевать эти сертификаты во исполнение требований потребителей облачных услуг.

Поставщикам облачных услуг следует обеспечить прохождение своим инженерным и другим персоналом учебных курсов по безопасности, а также получение им соответствующей квалификации для эксплуатации облачной вычислительной платформы.

7.2.2.8 Документирование мероприятий по обеспечению безопасности

Поставщики облачных услуг могут представлять документальные подтверждения своих усилий, направленных на повышение безопасности предоставляемой облачной услуги. Это могут быть документы с описанием принятых мер безопасности, процедурного регламента управления безопасностью и т. д. Следует обеспечить удобный доступ к этим документам с возможностью просмотра на веб-портале поставщика или загрузки оттуда.

8 Руководящие указания по обеспечению эксплуатационной безопасности в повседневной деятельности

Поставщикам облачных услуг следует принять меры и организовать мероприятия по обеспечению безопасности в рамках повседневной деятельности администраторов и групп внутренних пользователей. За счет указанных мер и мероприятий должно обеспечиваться выполнение поставщиками облачных услуг положений пункта о безопасности в соглашении об уровне обслуживания. Эти меры и мероприятия включают среди прочего следующие элементы.

1) **Меры безопасности**. Поставщики облачных услуг обязаны выполнить комплекс мер безопасности, предоставляющий основные возможности и средства для обеспечения эксплуатационной безопасности облачных вычислений.

   a) Управление определением идентичности и контроль доступа (пункт 8.1).

   b) Шифрование данных и управление ключами (пункт 8.2).

   c) Мониторинг безопасности системы (пункт 8.3).

   d) Восстановление после чрезвычайных ситуаций (пункт 8.4).

   e) Управление конфигурацией системы безопасности (пункт 8.5).

2) **Мероприятия по обеспечению безопасности**. Поставщики облачных услуг обязаны проводить регулярные мероприятия, направленные на решение проблем безопасности и обеспечение защищенности облачной вычислительной системы в процессе эксплуатации.

   a) Обработка событий, связанных с безопасностью (пункт 8.6).

   b) Внесение исправлений (пункт 8.7).

   c) Обеспечение безопасности управления конфигурацией (пункт 8.8).

   d) Планы реагирования на чрезвычайные ситуации (пункт 8.9).

   e) Резервное копирование (пункт 8.10).

   f) Внутренний аудит безопасности (пункт 8.11).

8.1 Управление определением идентичности и контроль доступа

8.1.1 Управление определением идентичности

Поставщикам облачных услуг следует обеспечить единое управление определением идентичности для внутренних администраторов и групп внешних пользователей, которые могут направлять необработанные данные для единого контроля доступа, авторизации и аудита.

1) Следует обеспечить поддержку федеративного определения идентичности для совместного использования учетных данных и синхронизации между различными облачными приложениями в одной зоне доверия.

2) Следует обеспечить поддержку управления жизненным циклом идентичности на всем его протяжении, включая реестр идентификационных данных, назначение ролей и привилегий, изменение привилегий, удаление идентификационных данных и т. д. При этом следует установить порядок, согласно которому регистрация и изменение идентификационных данных утверждаются администраторами.

3) К сфере политики управления определением идентичности относятся политика наименования идентификационных учетных записей, политика их применения и т. д. В этом комплексе сферы политики безопасности следует предусмотреть:

   - уникальность имени идентификационной учетной записи в пределах одной зоны доверия.
   - блокировку идентификационной учетной записи при многократном неправильном вводе пароля;
   - отключение идентификационной учетной записи при ее длительном неиспользовании;
   - запрет идентификационной учетной записи при многократных попытках входа в систему на протяжении очень короткого периода времени.

4) В рамках единого управления учетными записями пользователей следует точно связывать учетную запись с конкретными лицами или группой внутренних пользователей. Идентифицировать пользователей следует по основной учетной записи, которая должна быть в единственном числе у каждого пользователя (администратора или группы внутренних пользователей). В рамках основной учетной записи может быть создана подчиненная учетная запись, которой можно предоставить привилегии на управление ячейками сети, серверами баз данных, серверами приложений и т. д.

5) В рамках единого аудита учетных записей основное внимание следует уделять присваиванию идентификационной учетной записи, а также логике входа в систему и выхода из нее, диктуемой модулями контроля доступа. Это может помочь в обнаружении несанкционированно созданных и своевременно не удаленных учетных записей, учетных записей с избытком и недостатком полномочий, а также в предотвращении попыток входа в систему с вышедших из употребления или фальсифицированных учетных записей. В ходе аудита следует уведомлять модуль или системы аудита безопасности о событиях, связанных с безопасностью учетных записей, для выполнения более широкого спектра аудиторских функций, таких как обнаружение проникновений, мониторинг сбоев и т. д.

6) Следует обеспечить поддержку управления паролями пользователей, в том числе единых наборов стратегий управления паролями на основе правил безопасности облачной платформы, определяющих алгоритмы шифрования, длину пароля, его сложность и длительность цикла смены паролей. При этом следует предусмотреть поддержку паролей различных типов – графических, звуковых и т. д. Наконец, следует обеспечить поддержку синхронизации и сброса паролей.

7) Следует предоставить группам внутренних пользователей некоторые возможности самостоятельного управления учетными записями. Некоторые функции по управлению, такие как изменение ряда простых свойств пользователей и смена паролей, могут выполняться самими группами внутренних пользователей, что может облегчить бремя административного персонала по обслуживанию учетных записей.

8.1.2 Управление контролем доступа

Поставщикам облачных услуг следует создать единую централизованную систему аутентификации и авторизации для повышения безопасности контроля доступа в повседневной деятельности. Следует обеспечить ведение журналов контроля доступа в облачные вычислительные системы для последующего аудита.

1) Ниже перечислены функции, поддержку которых следует обеспечить в единой системе аутентификации:

- однократная регистрация входа (SSO) – следует предусмотреть установку параметров SSO, таких как максимальная длительность сеанса, максимальное время бездействия и максимальное время жизни кэша;
- общераспространенные технологии аутентификации, такие как LDAP, аутентификация по цифровому сертификату, аутентификация по жетону, биометрическая аутентификация, многофакторная аутентификация и т. д.;
- ведение подробных журналов аутентификации. Сюда входят системная идентификация; пользователи, входящие в систему и выходящие из нее; время входа; время выхода; IP-адрес входа; терминал входа; результаты входа (успешно или нет);
- дифференцированные дополнительные методы аутентификации для различных систем и услуг. Это позволяет соблюсти баланс между безопасностью и простотой в использовании и даже издержками.

2) Ниже перечислены функции, поддержку которых следует обеспечить в единой системе авторизации:

- авторизация для доступа к облачным ресурсам в зависимости от предварительного определения пользователей, групп пользователей и уровня привилегий;
- поддержка механизмов централизованной и иерархической авторизации, а также ограничение диапазона возможностей авторизации администраторов в иерархической системе со стороны администратора авторизации;
- стратегии авторизации с высоким и низким уровнями детализации;
- ведение подробных журналов авторизации с регистрацией IP-адресов, оператора, времени авторизации, а также предоставленных и отозванных разрешений.

3) Прочие требования:

- контроль доступа к журналам. Поставщикам облачных услуг следует обеспечить возможность доступа администраторов к журналам только при наличии соответствующих привилегий. Следует предусмотреть предоставление администраторами привилегий группам внешних пользователей для просмотра относящихся к ним журналов через веб-сайт портала самообслуживания или другие клиентские средства;
- механизмы шифрования. Критичные данные, такие как данные аутентификации, данные авторизации и т. п., следует шифровать в процессе хранения и передачи;
- надлежащий доступ для просмотра ко всем эксплуатационным журналам, касающимся потребителей облачных услуг.

8.2 Шифрование данных и управление ключами

Шифрование и управление ключами – основополагающие механизмы защиты данных в облачных вычислительных системах. Шифрование позволяет защищать ресурсы, а управление ключами обеспечивает контроль над ключами шифрования, используемыми для такой защиты.

В пункте соглашения об уровне обслуживания, регулирующем вопросы безопасности, следует четко определить конкретную реализацию алгоритма шифрования. Кроме того, используемое шифрование должно соответствовать применимым отраслевым и государственным стандартам. Поставщикам или потребителям облачных услуг следует серьезно рассмотреть следующие элементы:

1) шифрование данных при передаче по сети. Особенно важно защитить учетные данные, такие как финансовые реквизиты, пароли и т. д.;
2) шифрование статических данных на диске или в базе данных. Это помогает предотвратить злоумышленные действия со стороны поставщиков облачных услуг или других групп внутренних пользователей;
3) шифрование данных на резервных носителях. Это помогает предотвратить утечку данных в случае утери или кражи резервных носителей.

Если основные усилия по шифрованию данных прикладывает поставщик облачных услуг, важнейшей составляющей его повседневной деятельности является управление ключами. Поставщику облачных услуг следует разработать и внедрить комплексную систему управления жизненным циклом ключей, учитывая их генерацию, использование, хранение, резервное копирование, смену и уничтожение. Кроме того, поставщикам облачных услуг целесообразно уделить внимание следующим вопросам:

1) защита хранения ключей. Хранение ключей должно быть защищено наряду с хранилищами других критичных данных или даже более надежно. Доступ к хранению ключей должен предоставляться только конкретному объекту. Требуются также сопутствующие стратегии, такие как разделение ролей для более строгого контроля доступа;
2) резервное копирование и восстановление. Поскольку неожиданная потеря определенного ключа может сделать невозможным предоставление услуги, необходимо реализовать решения для резервного копирования и восстановления ключей;
3) стороннее управление ключами. Разделение задач может помочь поставщикам облачных услуг соблюсти законодательные требования в том случае, когда заявленное содержание услуги предусматривает предоставление данных в облачных вычислительных системах.

8.3 Мониторинг безопасности системы

В ходе повседневной деятельности поставщикам облачных услуг следует осуществлять в режиме реального времени централизованный мониторинг безопасности облачной платформы и инфраструктуры, включая состояние функционирования различных физических и виртуальных ресурсов. Руководствуясь ключевыми параметрами соглашения об уровне обслуживания (такими как производительность сети, использование ресурсов и хранилищ узла и т. д.) и анализируя всевозможные журналы, поставщики облачных услуг могут выявлять и устранять неисправности,

управлять качеством работы, а также управлять автоматическим наблюдением в целях обеспечения мониторинга работоспособности облачных ресурсов в реальном или квазиреальном времени.

Как правило, журналы мониторинга ведутся в строго конфиденциальном режиме поставщиками облачных услуг. Вместе с тем в случае необходимости поставщики облачных услуг могут предоставлять потребителям соответствующие журналы по требованию – например, для диагностики и устранения неисправностей в чрезвычайных ситуациях.

Поставщики облачных услуг также могут заранее выявлять потенциальные эксплуатационные риски и своевременно их устранять. Кроме того, поставщикам облачных услуг следует предоставить потребителям облачных услуг возможности для сравнительного анализа данных о потребителях и предоставляемых им услугах, что позволило бы диагностировать качество и безопасность облачных услуг.

Существует два режима мониторинга безопасности – автоматический мониторинг и визуальный контроль. Тот и другой опираются на технические средства и возможности управления, которыми располагают отдельные поставщики облачных услуг. В объем понятия мониторинга безопасности входят:

1) мониторинг работоспособности инфраструктуры облачных вычислений. Поставщикам облачной инфраструктуры следует предусмотреть возможность ведения и мониторинга журналов событий, связанных с безопасностью, а также мониторинга информации об уязвимостях, изменения конфигурации устройств обеспечения безопасности, качества работы и состояния функционирования всех объектов инфраструктуры облачных вычислений, включая ресурсы виртуальных машин, платформу управления облачными вычислениями, устройства обеспечения безопасности, базу данных и т. д. Такой мониторинг поможет поставщикам облачной инфраструктуры быть постоянно осведомленными об общем состоянии работоспособности и функционирования облачной инфраструктуры;

2) выявление аномальных действий. Аномальные действия включают несанкционированный вход в систему, несанкционированный доступ к платформе управления облачными вычислениями, неправомерный доступ к другим ресурсам, аномальные изменения в конфигурации сетевого оборудования и виртуальных машин, другие атаки с проникновением. Такие действия могут быть выявлены с использованием технических средств, таких как интегрированные средства аудита, программного обеспечения для предотвращения утечки данных или других средств обеспечения безопасности;

3) мониторинг аномального сетевого трафика. Поставщики облачных услуг должны располагать возможностями для обнаружения и анализа необычного трафика в физических и виртуальных сетях, особенно внутри виртуальных машин. Необходимо наличие постоянной осведомленности о сетевом трафике и качестве работы – это поможет поставщикам облачных услуг повысить уровень защищенности от компьютерных червей, атак на основе аномального трафика и других потенциальных угроз безопасности в среде облачных вычислений;

4) мониторинг физической безопасности. Объектами мониторинга физической безопасности являются система регулирования микроклимата, система видеонаблюдения (CCTV), пропускной пункт, система противопожарной защиты, кондиционер, система питания, система наблюдения, защитные каркасы и т. д., которые могут осматриваться ежедневно.

Прежде всего поставщикам облачных услуг следует выполнить полномасштабную проверку среды облачных вычислений для определения работоспособности облачных вычислительных служб в ходе повседневной работы и обслуживания. Это поможет быстро отслеживать различные показатели, такие как качество работы сети и виртуальных машин, качество оказания облачных услуг потребителям и т. д. Кроме того, для проведения такой проверки можно настроить оповещение о достижении пороговых или даже базисных значений. Собранная информация должна позволить поставщикам облачных услуг быстро диагностировать неисправности в сети, в хранилищах данных, на физических компьютерах и на виртуальных машинах в случае отказа.

Поставщики облачных услуг должны также располагать возможностями для выявления потребителей облачных услуг, которых мог затронуть отказ, методом сравнительного анализа, исходя из предположения об идентичности слабых мест, приложений, версий ОС и других факторов у потребителей.

8.4 Восстановление после чрезвычайных ситуаций

Поставщикам облачных услуг следует принять меры к восстановлению безопасности систем после чрезвычайных ситуаций до исходного уровня. Такие меры включают кластеризацию серверов, а также синхронное и асинхронное удаленное зеркальное копирование для "горячего" резервирования в ходе восстановления после чрезвычайных ситуаций.

1) Кластеризация серверов

   Кластеризация серверов обеспечивает согласованное реагирование на ошибки и отказы разных компонентов, а также прозрачное добавление компонентов в кластер с необходимой адаптационной способностью и масштабируемостью для достижения достаточной производительности.

2) Синхронное удаленное зеркальное копирование

   С помощью программного обеспечения для удаленного зеркального копирования данные с основной площадки синхронно реплицируются и передаются на удаленную площадку. В случае сбоя на основной площадке работающие программы переключаются на удаленную площадку. Синхронное удаленное зеркальное копирование позволяет обеспечить непрерывность деятельности без потери данных. Стоимость этого метода высока, так как для него необходимы сложное программное обеспечение и достаточно широкая полоса пропускания сети. Синхронное удаленное зеркальное копирование обычно реализуется в системах с высоким уровнем безопасности.

3) Асинхронное удаленное зеркальное копирование

   Существует и другой метод удаленного зеркального копирования, который обычно сопряжен с меньшими издержками, чем синхронное удаленное зеркальное копирование. При таком методе данные с основной площадки периодически реплицируются и передаются на удаленную площадку. В отсутствие сбоев можно гарантировать создание полной копии на резервной площадке без снижения качества работы основной площадки. Но если во время зеркального копирования происходит сбой, потеря данных неизбежна. Выбор в пользу асинхронного удаленного зеркального копирование целесообразно делать после достаточно тщательной оценки рисков.

8.5 Управление конфигурацией системы безопасности

Конфигурация системы безопасности включает правила безопасности, заданные в облачной платформе, сети, виртуальных машинах и в различных компонентах приложений. Она отличается от высокоуровневой политики безопасности, которая отражает подход организации к достижению поставленных целей в области безопасности.

Поставщикам облачных услуг следует осуществлять комплексное управление конфигурацией системы безопасности для ее эффективного внедрения и быстрого развертывания.

Предполагается, что в ходе этого процесса поставщики облачных услуг задают шаблоны и базовые конфигурации системы безопасности. Кроме того, поставщикам облачных услуг следует принимать меры к обеспечению внутренней согласованности и эффективности конфигурации системы безопасности при изменениях в облачной среде, а также к разделению конфигурации системы безопасности разных потребителей облачных услуг в среде с множественной принадлежностью.

Шаблоны конфигурации системы безопасности – это основные шаблоны, необходимые в текущей реализации облачной вычислительной среды, например шаблоны управления учетными записями, аутентификации, стратегий контроля доступа, политики аудита, политики динамического реагирования, политики обновления прикладного и системного программного обеспечения, политики резервного копирования и восстановления и т. д.

Базовые конфигурации системы безопасности задают требования ко всей облачной вычислительной среде, исходя из которых поставщики облачных услуг могут оценить, соответствует ли текущая конфигурация системы безопасности необходимому базовому уровню безопасности, а также определить детальный перечень мер для повышения уровня безопасности. Среди прочего, базовые конфигурации системы безопасности следует устанавливать для ОС, баз данных, брандмауэров, коммутаторов и маршрутизаторов.

Управление конфигурацией системы безопасности включает в себя следующие меры:

1) Управление шаблонами конфигурации системы безопасности

Поставщикам облачных услуг следует задать основные шаблоны безопасности для нужд облачной среды в целях ускорения и облегчения развертывания конфигурации системы безопасности. В рамках управления шаблонами конфигурации системы безопасности следует обеспечить поддержку настраиваемых шаблонов, а также непрерывное обновление и оптимизацию шаблонов в соответствии с изменениями в облачной платформе, состоянии сети, требованиях к обслуживанию и т. д.

Кроме того, поставщикам облачных услуг следует предусмотреть для потребителей облачных услуг возможность настраивать новые шаблоны конфигурации системы безопасности в соответствии с собственными требованиями. При этом потребители облачных услуг должны самостоятельно нести ответственность за эффективность настроенной ими конфигурации системы безопасности.

2) Процесс управления конфигурацией системы безопасности

Поставщикам облачных услуг следует засвидетельствовать эффективность используемой конфигурации системы безопасности. Конфигурация системы безопасности может настраиваться в соответствии с требованиями потребителей облачных услуг и потребностями самих этих услуг. Основной процесс управления конфигурацией системы безопасности включает в себя запрос на изменение конфигурации, утверждение изменения конфигурации, тестирование и техническую проверку, реализацию, архивирование конфигурации и составление отчета.

3) Управление базовыми конфигурациями системы безопасности

Поставщикам облачных услуг следует разработать базовые конфигурации системы безопасности, обеспечив всесторонний учет требований к безопасности облачной вычислительной платформы, облачных услуг и потребителей облачных услуг, положений пункта о безопасности в соглашении об уровне обслуживания и т. д.

Основной процесс управления базовыми конфигурациями системы безопасности включает в себя запрос на проверку конфигурации системы безопасности, ее документирование, утверждение, выполнение проверки, составление отчета о проверке, принятие мер к повышению безопасности и составление отчета о принятых мерах. Проверку конфигурации системы безопасности следует выполнять периодически в ходе повседневной работы и можно реализовать путем сбора данных о конфигурации и проверки обеспечения базового уровня безопасности.

4) Управление конфликтами в конфигурации системы безопасности

В облачной среде с совместным использованием ресурсов возможны ошибки в конфигурации системы безопасности по вине администратора безопасности или по другим причинам. Они в свою очередь могут привести к возникновению уязвимостей в облачной вычислительной среде. Поставщикам облачных услуг следует принять эффективные меры к выявлению конфликтов в конфигурации системы безопасности и установить процесс разрешения таких конфликтов.

Процесс разрешения конфликтов в конфигурации системы безопасности должен включать оповещение о конфликте, анализ конфликта (с определением причин и влияющих факторов), действия по разрешению конфликта и составление отчета.

5) Управление корректировкой конфигурации системы безопасности

Поставщикам облачных услуг следует предусмотреть способы динамической корректировки конфигурации системы безопасности при изменениях, затрагивающих облачный вычислительный ресурс или услугу (например, при повышении нагрузочной способности, миграции виртуальной машины и т. д.). Например, на случай миграции виртуальной машины можно предусмотреть автоматическую миграцию политики конфигурации системы безопасности посредством мониторинга состояния миграции, автоматического сопоставления и повторного развертывания исходной политики конфигурации системы безопасности. Тем самым можно обеспечить внутреннюю согласованность политики конфигурации системы безопасности и быстрое ее развертывание в облачной среде, а также повысить эффективность процесса обеспечения безопасности.

6) Управление разделением конфигурации системы безопасности

В облачной среде с множественной принадлежностью поставщикам облачных услуг следует строго управлять классификацией конфигурации систем безопасности потребителей облачных услуг, а также принимать меры по аутентификации, контролю доступа и т. д. Это необходимо для разделения конфигурации систем безопасности различных потребителей облачных услуг.

8.6 Обработка событий, связанных с безопасностью

Поставщикам облачных услуг следует проводить определенные мероприятия по обработке событий, связанных с безопасностью облачной вычислительной среды, например оповещений об угрозах, уязвимостях, экстренных ситуациях и т. д. Кроме того, им следует принимать технические меры, помогающие в выявлении событий, связанных с безопасностью, оповещении о таких событиях и их обработке.

В общем случае процесс обработки событий, связанных с безопасностью, в облачной вычислительной среде включает в себя следующие этапы: выявление, анализ, реагирование, проверку, составление отчета и документирование. Поставщикам облачных услуг следует отчетливым образом назначить лиц, ответственных за каждый из этапов.

8.6.1 Выявление

Поставщикам облачных услуг следует принимать меры для мониторинга состояния безопасности облачной платформы, перечисленные в пункте 8.3, располагать возможностями для своевременной рассылки оповещений о событиях, связанных с безопасностью. Им следует обеспечить возможность направления оповещений назначенному лицу – например, менеджеру по безопасности облачной вычислительной платформы. Для рассылки оповещений могут использоваться электронная почта, телефон, SMS и другие каналы. Поставщикам облачных услуг следует обеспечить мониторинг всех связанных с безопасностью событий, предусмотренных пунктом о безопасности в соглашении об уровне обслуживания.

8.6.2 Анализ

После получения оповещений о событиях, связанных с безопасностью, поставщикам облачных услуг следует убедиться в их достоверности, а затем провести анализ и диагностику для классификации событий, определения их причин и выработки мер реагирования. При необходимости поставщики облачных услуг могут обращаться за содействием к потребителям облачных услуг.

8.6.3 Реагирование

Поставщикам облачных услуг следует принимать меры реагирования на события, связанные с безопасностью, в соответствии с их типом и степенью серьезности, с тем чтобы минимизировать последствия этих событий. Реагирование включает мероприятия по обеспечению безопасности, перечисленные в пунктах 8.7, 8.8 и 8.9, в том числе:

1) в случае чрезвычайной ситуации в области безопасности поставщикам облачных услуг следует предпринять действия в соответствии с планами реагирования на чрезвычайные ситуации;

2) в случае уязвимости в системе безопасности поставщикам облачных услуг следует предпринять действия по внесению исправлений;

3) в случае недочета в конфигурации поставщикам облачных услуг следует предпринять действия по управлению конфигурацией системы безопасности.

Поставщикам облачных услуг следует обеспечить мониторинг и оценку событий, связанных с безопасностью, в динамическом режиме, а также информирование потребителей облачных услуг (в том числе о ходе реализации мер реагирования).

8.6.4 Проверка

После реализации мер реагирования на события, связанные с безопасностью, поставщикам облачных услуг следует подробнее проанализировать причины и обстоятельства этих событий и проверить, нет ли в системах других потребителей облачных услуг схожих уязвимостей, которые могли бы привести к тем же событиям. Если такие уязвимости существуют, поставщикам облачных услуг следует немедленно уведомить об этом потребителей облачных услуг и принять соответствующие меры. Такое уведомление не должно нарушать конфиденциальность данных других потребителей облачных услуг.

8.6.5 Составление отчета и документирование

Поставщикам облачных услуг следует составить отчет об обработке событий, связанных с безопасностью, в котором должны излагаться суть события, его причины, меры реагирования и т. д. Отчет следует направить потребителям облачных услуг, затронутым этими событиями, в сроки, предусмотренные пунктом о безопасности соглашения об уровне обслуживания. Информацию о событиях, связанных с безопасностью, следует задокументировать для дальнейшего контроля и аудита. Соответствующие отчеты могут представляться потребителям облачных услуг, затронутым этими событиями, и сторонним аудиторам, действующим в качестве партнера по облачной услуге).

8.7 Внесение исправлений

8.7.1 Распределение обязанностей

Поставщикам облачных услуг следует оптимизировать процесс управления внесением исправлений в облачную платформу в целях снижения рисков, связанных с уязвимостями, и обеспечить стабильную работу облачных платформ и услуг.

В сфере облачных вычислений обязанности по управлению внесением исправлений следует распределить между поставщиками и потребителями облачных услуг.

1) Обязанности поставщика облачных услуг:
   - отслеживание публикации сведений об уязвимостях зеркальных операционных систем и своевременное нахождение новейших исправлений;
   - тестирование безопасности и совместимости исправлений;
   - обновление исправлений зеркальных операционных систем и создание новейших обновленных файлов образов;
   - информирование потребителей облачных услуг об исправлениях, содействие им в завершении установки исправлений и предотвращение возникновения аналогичной уязвимости;
   - тестирование результатов установки исправлений на обновленных файлах образов путем создания новой виртуальной машины.
2) Обязанности потребителя облачных услуг:
   - содействие поставщикам облачных услуг в отслеживании публикации сведений об уязвимостях и в поиске новейших исправлений;
   - своевременное внесение исправлений в виртуальные машины согласно информации, полученной от поставщиков облачных услуг.

В зависимости от режима предоставления облачных услуг (IaaS, PaaS или SaaS) поставщик облачных услуг, как и потребитель, отвечает только за те ресурсы, которые находятся под его контролем. В случае IaaS поставщик облачных услуг должен также отвечать за внесение исправлений в облачную вычислительную инфраструктуру, а потребитель облачных услуг – за внесение исправлений в гостевую ОС, прикладное программное обеспечение и другие ресурсы, находящиеся под его контролем.

8.7.2 Процесс внесения исправлений в систему безопасности

Во внесении исправлений могут нуждаться, в частности, такие компоненты облачной платформы, как программное обеспечение для виртуализации, операционные системы, сетевое оборудование, оборудование безопасности, серверы баз данных, терминалы управления. Циклический процесс внесения исправлений состоит из четырех этапов. Этот процесс, описанный ниже, поможет поставщикам облачных услуг наиболее эффективно обеспечить своевременное внесение исправлений в свою платформу.

1) Сбор исправлений

Поставщикам облачных услуг следует собирать информацию об исправлениях с официальных веб-сайтов поставщиков соответствующих продуктов, использовать предоставленные поставщиками автоматические средства внесения исправлений или другими способами обеспечивать соблюдение требований к внесению исправлений. Поставщикам облачных услуг следует анализировать собранные исправления, искать и документировать уязвимости существующих систем и приложений, оценивать возможные последствия и риски внесения исправлений, а также определять степень срочности и важности исправлений.

2) Тестирование исправлений

Поставщикам облачных услуг следует организовать тестирование исправлений для проверки их безопасности, совместимости и стабильности. Для этого следует создать тестовую среду, которая бы эмулировала целевую платформу или системы в состоянии до внесения исправлений. По результатам испытания следует составить отчет с заключением о том, следует ли вносить исправления. В отчете следует также привести подробные пошаговые технические указания по внесению исправлений и откату к исходному состоянию. Отчет должен содержать полное описание исправлений, которое давало бы специалистам представление об их функциональности и принципах работы, а также о последствиях, которые внесение этих исправлений повлечет для различных систем и приложений, например о создаваемых исправлением проблемах, затрагиваемых файлах, необходимости перезагрузки системы или приложения и т. д.

3) Внесение исправлений

Поставщикам облачных услуг следует разработать подробный пошаговый план действий по внесению исправлений, исходя из отчета о результатах их тестирования. Следует также разработать план действий в экстренной ситуации, включающий резервное копирование системы и данных, переключение приложений, удаление исправления и откат системы к исходному состоянию в случае сбоя, вызванного исправлением. Если предстоит внести крупномасштабные исправления, поставщикам облачных услуг следует заблаговременно обратиться за технической поддержкой к поставщикам соответствующего программного обеспечения в целях повышения эффективности действий в непредвиденных ситуациях.

Поставщикам облачных услуг также следует уведомлять потребителей облачных услуг о сроках внесения исправлений в облачную платформу и четко предупреждать их перед внесением исправлений. Поставщикам облачных услуг не следует пытаться каким бы то ни было образом повлиять на предоставляемые потребителям облачные услуги – необходимо принимать надлежащие меры в сотрудничестве с потребителями облачных услуг.

4) Проверка исправлений

После внесения исправлений поставщикам облачных услуг следует регулярно проверять актуальность внесенных исправлений в масштабах всей облачной платформы с помощью средств управления внесением исправлений. Документы о внесении исправлений следует регулярно обновлять и архивировать для последующего аудита безопасности.

Время ожидания с момента получения информации о выходе исправления до момента внесения этого исправления, а также требование санкции на его внесение со стороны потребителя облачной услуги следует отчетливо оговорить в соглашении об уровне обслуживания исходя из приоритета исправления (критический, высокий, средний и низкий).

На рисунке ниже показан пример процесса внесения исправлений в систему безопасности, включающий обновление виртуальной машины и ее файлов образа. Процесс протекает следующим образом. Если выпущены новые исправления, поставщики облачных услуг тестируют безопасность и совместимость этих исправлений. Потребители облачных услуг несут обязанности по поиску и сбору последних исправлений. После успешного тестирования последних исправлений поставщики облачных услуг дают потребителям облачных услуг указание внести эти исправления. Одновременно поставщики облачных услуг вносят те же исправления в действующие файлы образов. После этого поставщики облачных услуг могут создать новую виртуальную машину с использованием полученных файлов образов. Поставщики облачных услуг также обеспечивают проверку успешного внесения исправлений потребителями облачных услуг.

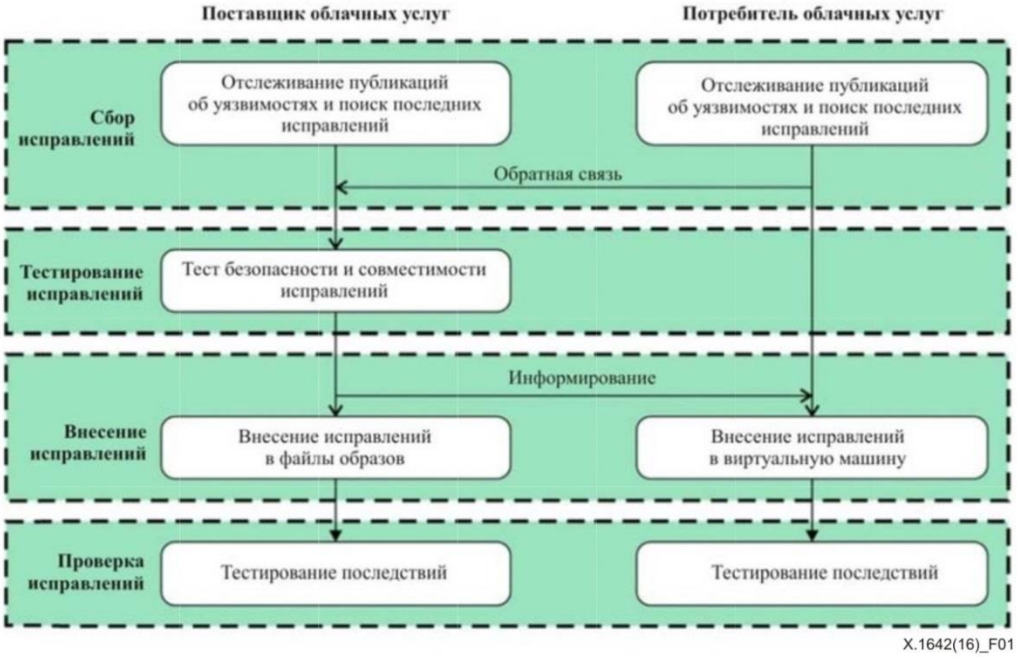

Рисунок 1 – Пример процесса внесения исправлений в систему безопасности

8.8 Обеспечение безопасности управления конфигурацией

Поставщикам облачных услуг следует обеспечивать безопасность управления конфигурацией облачной платформы и конфигурацией сети, а также параметрами различных компонентов приложений, что поможет снизить эксплуатационные риски, обусловленные неправильной конфигурацией или ненадлежащим использованием, и повысить безопасность и стабильность облачной вычислительной среды.

Управление конфигурацией обычно включает в себя управление внесением изменений в конфигурацию и управление выпусками. Поставщикам облачных услуг следует принимать меры для обеспечения мониторинга и документирования выпусков и изменений в конфигурации. Для удобства управления конфигурацией обычно создается специальная интегрированная база данных, в которой хранится информация о текущих и предшествующих версиях всех конфигурационных файлов, политики безопасности, прикладных профилей каждого элемента и компонента облачной вычислительной системы. Поставщикам облачных услуг следует защищать базу данных управления конфигурацией от несанкционированного доступа, утечки информации и т. д.

Обеспечение безопасности управления конфигурацией включает в себя следующее.

1) Аудит управления конфигурацией

Аудит управления конфигурацией призван обеспечить эффективное выполнение требований к изменениям в конфигурации и выпускам. Он помогает поставщикам облачных услуг проверять корректность, внутреннюю согласованность, полноту, действительность и прослеживаемость каждого элемента конфигурации. Аудит управления конфигурацией следует проводить периодически в ходе повседневной деятельности.

Все журналы доступа пользователей, изменений, архивирования и извлечения следует сохранять и архивировать для аудита в составе работающей системы или в автономном режиме.

Кроме того, потребителям облачных услуг следует предоставить надлежащий доступ к отчету о результатах аудита управления конфигурацией в отношении этих потребителей или предоставляемых им услуг, с тем чтобы у потребителей облачных услуг была возможность надзора за мерами безопасности и эффективностью работы поставщиков облачных услуг.

2) Мониторинг управления конфигурацией

Поставщикам облачных услуг следует вести мониторинг изменений в конфигурационных файлах и других действий с этими файлами в масштабах всей облачной вычислительной среды для предотвращения несанкционированного доступа, утечки данных, неправомерного внесения изменений и ошибок в конфигурации.

3) Защита базы данных управления конфигурацией

Поставщикам облачных услуг следует тщательно обслуживать базу данных управления конфигурацией и управлять ею, в том числе осуществляя авторизацию на основе ролей, удаление ненужных данных, регулярный аудит, периодическое резервное копирование и т. д.

8.9 Планы реагирования на чрезвычайные ситуации

Чрезвычайно важно обеспечить, чтобы после случившегося инцидента в области безопасности поставщики облачных услуг могли эффективно эксплуатировать облачные вычислительные системы без избыточных перебоев в работе. Это обеспечивается с помощью плана реагирования на чрезвычайные ситуации, устанавливающего эффективную программу и порядок действий, а также технические меры реагирования.

В целях смягчения последствий инцидентов в сфере безопасности для облачных вычислительных платформ и услуг составленный поставщиком облачных услуг план реагирования на чрезвычайные ситуации должен содержать четкие руководящие указания для операторов при обеспечении баланса между уровнем детализации и степенью гибкости. Разработка и корректировка плана реагирования на чрезвычайные ситуации – это циклический процесс непрерывного совершенствования, состоящий из трех фаз: фазы разработки, фазы тестирования и внедрения и фазы поддержания.

8.9.1 Фаза разработки

Прежде всего необходимо внедрить методы качественного и количественного анализа для комплексной оценки рисков, связанных с облачными вычислительными системами, а также анализа последствий для деятельности (BIA) в связи с их использованием. По итогам такого анализа можно определить основные особенности и компоненты системы, а также последствия различных инцидентов безопасности. На этой основе в соответствии с требованиями пункта о безопасности в соглашении об уровне обслуживания между поставщиком и потребителем облачных услуг и нормативными требованиями можно установить целевые параметры восстановления после чрезвычайной ситуации, такие как целевые сроки восстановления (RTO) и целевая точка восстановления (RPO). Кроме того, при разработке плана реагирования на чрезвычайные ситуации следует принимать во внимание характер облачных услуг и классификацию инцидентов.

План реагирования на чрезвычайные ситуации включает:

1) уведомление. Следует разработать порядок уведомления группы реагирования, руководства и затронутых потребителей облачных услуг в случае инцидента безопасности;

2) классификацию и ранжирование инцидентов безопасности. Следует обеспечить классификацию и ранжирование инцидента безопасности группой реагирования на чрезвычайные ситуации;

3) запуск программы реагирования. По итогам классификации и ранжирования инцидентов безопасности поставщикам и потребителям облачных услуг необходимо срочно запустить разработанную ранее соответствующую программу реагирования;

4) принятие мер. После запуска программы реагирования следует немедленно приступить к реализации мер по смягчению последствий инцидента безопасности. Кроме того, сразу после того, как инцидент будет взят под контроль, следует начать восстановление;

5) оценку. После принятия мер для устранения чрезвычайной ситуации важно сделать соответствующие выводы по ее итогам. В частности, следует проанализировать и сформулировать причины инцидента, оценить ущерб и эффективность плана реагирования на чрезвычайные ситуации.

Кроме того, первостепенную важность представляют следующие аспекты:

1) состав группы реагирования на чрезвычайные ситуации, распределение обязанностей в группе и контактные данные всех членов группы. Вообще говоря, группа реагирования на чрезвычайные ситуации состоит из представителей руководящего, коммерческого, технического и административного персонала;

2) результаты оценки последствий чрезвычайной ситуации для деятельности с учетом взаимосвязей между различными частями облачной вычислительной системы, приоритетом основных компонентов и другими факторами;

3) критерии, порядок и контрольные списки восстановления облачной вычислительной системы;

4) перечень аппаратного, программного, микропрограммного обеспечения и других ресурсов, играющих вспомогательную роль в повседневной деятельности поставщика облачных услуг, с указанием версий, количества и других параметров для каждой позиции;

5) контактные данные потребителей облачных услуг и порядок реагирования, согласованный поставщиками и потребителями облачных услуг в соответствии с пунктом о безопасности в соглашении об уровне обслуживания, в целях минимизации ущерба потребителя в случае инцидента безопасности;

6) в общем случае поставщик облачных услуг может не иметь привилегий для доступа к частным данным потребителя облачных услуг без разрешения последнего. Если программа реагирования на чрезвычайную ситуацию запущена потребителем облачных услуг, последний может нуждаться в помощи поставщика облачных услуг для повышения эффективности мер реагирования и в связи с этим дать поставщику разрешение на доступ к данным. Для обеспечения соответствия деятельности поставщика облачных услуг требованиям он не должен злоупотреблять разрешением на доступ к данным потребителя облачных услуг.

8.9.2 Фаза тестирования и внедрения

Для проверки эффективности плана реагирования на чрезвычайные ситуации поставщикам облачных услуг следует организовывать тестирование этого плана и учения по нему при содействии персонала, знакомого с порядком реагирования. К тестированию и учениям предъявляются следующие требования:

1) Программы тестирования, практических занятий и учений должны быть составлены заранее.

2) Процесс тестирования, практических занятий и учений должен быть подробно задокументирован с составлением соответствующих отчетов.

3) Поставщикам и потребителям облачных услуг рекомендуется проводить запланированное тестирование в масштабах организации всякий раз, когда в облачной вычислительной среде или за ее пределами происходят существенные изменения.

В случае инцидентов безопасности или перебоев в работе следует четко соблюдать план реагирования на чрезвычайные ситуации наряду с выполнением условий его ввода в действие, и все мероприятия на протяжении всего процесса ликвидации чрезвычайной ситуации должны быть запротоколированы. После этого поставщику облачных услуг следует отчитаться перед потребителями облачных услуг о принятых мерах реагирования в соответствии с положениями пункта о безопасности в соглашении об уровне обслуживания.

По результатам тестирования, учений и внедрения следует пересматривать план реагирования на чрезвычайные ситуации для повышения его действенности и реалистичности.

8.9.3 Фаза поддержания

Для сохранении эффективности плана реагирования на чрезвычайные ситуации следует постоянно поддерживать его в актуальном состоянии, отражающем требования облачных вычислительных систем, а также изменения в соглашении об уровне обслуживания, в конфигурации системы и в составе персонала. В общем случае план следует пересматривать ежегодно для учета фактических изменений в облачной вычислительной среде. Основания для корректировки плана включают:

1) изменения, касающиеся места осуществления деятельности, материально-технической базы, ресурсов и услуг.

2) изменения требований пункта о безопасности в соглашении об уровне обслуживания, изменения в критически важных элементах конфигурации системы безопасности, существенные исправления, изменения в составе ключевых участников коллектива;

3) результаты оценки эффективности плана по подробным документальным материалам о фактической реализации плана в ходе тестирования и в ответ на реальные инциденты безопасности.

8.10 Резервное копирование

Возможность резервного копирования – важный аспект для потребителей и поставщиков облачных услуг. Прежде чем приступать к мероприятиям по резервному копированию, поставщикам облачных услуг необходимо определить следующее:

– стратегию резервного копирования для каждого потребителя облачных услуг или конкретной облачной услуги;

– метод хранения, в том числе наличие или отсутствие шифрования;

– место хранения (в том числе локальное или удаленное);

– сроки хранения резервных копий данных;

– порядок тестирования резервных копий данных.

Прежде чем выбирать поставщика облачных услуг, потребителям облачных услуг следует выяснить, в состоянии ли поставщик выполнить требования пункта о безопасности соглашения об уровне обслуживания, касающиеся резервного копирования. Если поставщик облачных услуг не предоставляет возможность резервного копирования, потребителю следует в полном объеме рассмотреть вопросы о стратегии резервного копирования и ее реализации. Если же возможность резервного копирования предоставляется поставщиком облачных услуг, потребителю следует осуществлять резервное копирование во взаимодействии с поставщиком.

Поставщику облачных услуг следует информировать потребителей облачных услуг о важнейших аспектах механизма резервного копирования. При решении задач резервного копирования поставщикам облачных услуг следует определить перечисленные ниже аспекты этого процесса в соответствии с требованиями потребителей.

1) Стратегия резервного копирования. Поскольку у каждого потребителя облачных услуг имеются свои запросы в отношении резервного копирования, следует определить ряд сопутствующих параметров, в том числе:

- разумную целевую точку восстановления (RPO) и разумные целевые сроки восстановления (RTO). RPO определяет интервал времени между двумя последовательными операциями резервного копирования, а RTO – время отката к резервной копии;
- разумную политику хранения. Эта политика должна устанавливать количество хранимых резервных копий;
- разумное сочетание резервного копирования на уровне файлов и на уровне виртуальной машины. Это сочетание должно обеспечивать оптимальную стоимость инвестиций исходя из RPO и RTO;
- разумное сочетание локального и удаленного резервного копирования. Локальная резервная копия хранится на месте, что позволяет быстро произвести восстановление после чрезвычайной ситуации. Удаленная резервная копия хранится на удаленном сервере, что может быть необходимо для восстановления после крупномасштабного бедствия. Это сочетание зависит от требований пункта о безопасности соглашения об уровне обслуживания, а также от стоимости инвестиций;
- регулярное тестирование восстановления. Тестирование восстановления в конечном счете определяет пригодность резервной копии к использованию.

2) Организация выполнения задач резервного копирования. Определившись со стратегией, поставщикам облачных услуг следует надлежащим образом организовать выполнение задач резервного копирования. В целях ослабления влияния резервного копирования на качество работы инфраструктуры облачных вычислений следует организовать выполнение задач резервного копирования исходя из нужд потребителей облачных услуг, закономерностей изменения сетевого трафика и возможностей резервного копирования, которыми располагает поставщик.

3) Порядок проверки пригодности резервной копии к использованию. Полная и правильная копия данных свидетельствует об успехе операции резервного копирования. Как правило, проверка пригодности к использованию должна состоять из двух основных этапов:

- проверки соответствия резервной копии исходным данным с использованием односторонней хэш-функции. Если резервная копия совпадает с оригиналом, переходят к следующему этапу. Для проверки резервной копии можно также использовать метод цифровой подписи, что может дать некоторые дополнительные преимущества с точки зрения управления резервным копированием.
- теста восстановления из резервной копии. Ввиду постоянных изменений в облачной вычислительной среде крайне важно регулярно тестировать восстановление.

4) Осмотрительность в использовании моментальных снимков виртуальной машины. В облачной вычислительной среде метод моментальных снимков обеспечивает быстрый и легкий откат к исходному состоянию и таким образом в некоторой степени может служить методом резервного копирования. Однако методом моментальных снимков нецелесообразно пользоваться часто по следующим причинам:

- моментальные снимки дают возможность многократного дублирования одних и тех же данных с записью их в разные файлы снимков, что может привести к существенному ухудшению качества работы системы и стремительному снижению доступной емкости хранилищ облачной вычислительной системы.
- в целях повышения доступной емкости хранилищ зачастую делается цепочка моментальных снимков исходной виртуальной машины, каждый элемент которой содержит только изменения относительно первого снимка. После удаления первого моментального снимка все последующие снимки оказываются непригодны к использованию. Риск нарушения безопасности многократно возрастает с ростом частоты последовательно генерируемых снимков.

8.11 Внутренний аудит безопасности

Ввиду широты понятия аудита безопасности в настоящей Рекомендации рассматривается только внутренний аудит безопасности с точки зрения эксплуатационной безопасности. Надежный и объективный аудит безопасности поможет обеспечить тщательное тестирование и анализ деятельности по управлению эксплуатационными рисками, повысить уровень прозрачности облачных вычислительных служб и даже соблюсти нормативные требования.

8.11.1 Требования к аудиту безопасности

Для обеспечения объективности и надежности аудита безопасности поставщикам и потребителям облачных услуг следует прийти к соглашению об общей системе контроля и сертификации в области ИТ, а также о способах сбора, хранения и распространения аудиторского досье (системных журналов, отчетов о деятельности, конфигураций системы). Согласно положениям пункта о безопасности в соглашении о уровне обслуживания между поставщиком и потребителями облачных услуг аудит безопасности должен отвечать ряду требований:

1) Состав аудиторской группы и задачи аудита. Во-первых, в состав аудиторской группы должны входить высшие руководители и персонал различных отделов организации (административных и технических) для обеспечения объективности процесса аудита и возможности планирования ресурсов на его протяжении. Во-вторых, в задачи аудита должна входить проверка архитектуры управления безопасностью в организациях поставщика и/или потребителей облачных услуг, а также эффективности и правильности мер по управлению рисками. В-третьих, процесс аудита должен контролироваться аудиторской группой и соответствовать стандартам. Наконец, аудит должен выполняться регулярно с надлежащей периодичностью.

2) Требования к процессу аудита. Во-первых, исходя из вышесказанного выполняемые в рамках аудита действия должны документироваться в полном объеме и грамотно планироваться во избежание создания помех деятельности поставщика или потребителей облачных услуг. Во-вторых, следует четко определить круг задач аудита и необходимые для него ресурсы, а также гарантировать доступность этих ресурсов. Наконец, следует полностью задокументировать порядок проведения аудита и все требования к нему, а также обязанности членов аудиторской группы.

3) Защита средств аудита. Использование средств аудита следует ограничить и стандартизировать во избежание нецелевого использования ресурсов облачной вычислительной системы.

8.11.2 Специфические требования к аудиту

В отличие от порядка проведения аудита в традиционных информационных системах члены аудиторской группы должны быть знакомы со специфическими проблемами, связанными с виртуализацией и другими технологиями облачных вычислений. Вместе с тем предметом аудита помимо традиционных журналов безопасности становится работа с данными (в том числе деловыми), управление ими и даже место хранения пользовательских данных. К специфическим элементам аудита относятся, в частности:

1) аудит безопасности виртуализации. Основные требования аудита включают применение средств шифрования, проверку целостности файлов образов виртуальных машин, изоляцию и укрепление системы безопасности различных виртуальных машин, контроль доступа к виртуальным машинам, миграцию виртуальных машин, мониторинг процессов в виртуальных машинах, контроль виртуальных машин на предмет уязвимостей, мониторинг внутреннего трафика и меры безопасности в виртуальной сети;

2) аудит безопасности архитектуры и компонентов облачной платформы. Чрезвычайно важно проверить рациональность и эффективность реализуемых контрмер, включая политику разделения доменов безопасности, избыточность системы безопасности сетевой архитектуры и базовых компонентов, сканирование на предмет уязвимостей и укрепление системы безопасности, упаковку и распространение исправлений, конфигурацию системы предотвращения проникновений (IPS) и системы обнаружения проникновений (IDS), конфигурацию брандмауэров и устройств обеспечения безопасности при виртуализации;

3) аудит эксплуатации, обслуживания и деловой практики. Требования этого элемента аудита касаются главным образом документов об эксплуатации и обслуживании, журналов делового доступа, доступа к данным и анализа деловой практики;

4) аудит управления определением идентичности и доступом (IAM) и аудит контроля доступа. Требования этого элемента аудита важны для обеспечения правильного функционирования облачной вычислительной среды, включая проектирование и развертывание многофакторной аутентификации, контроль доступа, однократную регистрацию входа (SSO), разделение обязанностей и управление привилегированными пользователями;

5) аудит управления ключами и шифрования данных. Шифрование – базовый механизм защиты данных в облачной вычислительной среде вне зависимости от режима предоставления услуг (IaaS, PaaS или даже SaaS), поэтому среди прочего аудит должен предъявлять требования к реализации управления ключами и шифрования данных, а также к фактической обработке этих функций;

6) аудит системы реагирования и управления в чрезвычайных ситуациях. Требования этого элемента аудита касаются главным образом плана реагирования в чрезвычайных ситуациях, централизованного управления инцидентами безопасности и анализа корреляций между различными событиями, связанными с безопасностью.

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-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 г.) | ISO/IEC 17788:2014, *Информационные технологии – Облачные вычисления – обзор и словарь*.

[b-ITU-T Y.3510] Рекомендация МСЭ-Т Y.3510 (2016 г.), *Требования к инфраструктуре облачных вычислений*.

[b-ISO/IEC DIS 19086-1] ISO/IEC DIS 19086-1: 2016, *Information technology – Cloud computing – Service level agreement (SLA) framework and technology – Part 1: Overview and concepts*.

[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 DIS 27017] ISO/IEC DIS 27017:2015 , *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[b-ISO 27729] ISO 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

[b-NIST-SP-800-30] NIST Special Publication 800-30 Rev. 1 (2012), *Guide for Conducting Risk Assessments*.

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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2017 г.