СОВРЕМЕННЫЕ ПОДХОДЫ К КОМПЛЕКСНОМУ ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАКЕ

Савельев И.А.[1], Боровская О.Е.[2]

Ключевые слова: *информационная безопасность, подходы, облако, защита облака, облачные технологии, облачные сервисы, угрозы, провайдер, информатизация, программное обеспечение.*

Аннотация

Цель работы: обоснование продуктивного подхода к обеспечению информационной безопасности в облачных технологиях.

Методы исследования: системный и экспертный анализ механизмов защиты облачной инфраструктуры в целях устранения ее основных угроз, классификация применяемых облаков.

Результаты исследования: описаны подходы к защите облаков в зависимости от категории используемой инфраструктуры — частные/публичные облака; проведен сравнительный анализ разделения ответственности между провайдером и пользователем таких облачных сервисов, как IaaS, PaaS, SaaS — анализ показал, что компания обеспечивает защиту всех уровней облачной инфраструктуры самостоятельно в случае использования частного облака, в случае использования публичного облака — за компанией остается меньший контроль за защитой, что позволяет сэкономить денежные средства на обслуживающих специалистов, но лишает возможности вносить существенные изменения в текущую инфраструктуру для соответствия требованиям регуляторов.

Практическая значимость исследования подтверждается определением набора практических рекомендаций по устранению основных угроз облачной инфраструктуры путем применения средств защиты информации различных классов, примеры которых представлены в работе.

EDN: SCDBVL

Введение

В настоящее время объем облачных услуг в России интенсивно растет, проявляется тенденция сотрудничества международных компаний с провайдерами облачных сервисов. Это подтверждает международная исследовательская компания *IDC* (*International Data Corporation*) в своей работе «Рынок облачных услуг России перевалил за миллиард долларов»[3], а также статистика крупнейших интеграторов в сфере информационных технологий в связи с увеличением проектов, связанных с облачной средой.

История с пандемией КОВИД-19 подчеркивает, что бизнес-процессы в крупнейших предприятиях требуют такого уровня информатизации, чтобы у работников был доступ к ресурсам бизнес-процессов в любое время и из любой точки мира. Использование облачных технологий — то, что позволяет обеспечивать необходимый уровень доступности. Все это говорит о том, что вопросы *безопасности* облачных инфраструктур как никогда актуальны.

В рамках данной работы были поставлены следующие задачи:

- типизировать и классифицировать типы облаков;
- сформировать перечень наиболее актуальных угроз для частного и публичного облаков;
- определить наиболее актуальные угрозы, встречающиеся в частных и публичных облаках, и способы их устранения;
- выделить особенности разделения ответственности между провайдером и пользователем облачных сервисов;
- сформировать единый подход к обеспечению *информационной безопасности* (ИБ) [9] в облаке.

[3] URL: https:/www.idc.com/cis/research

[1] ***Савельев Иван Андреевич,*** *кандидат технических наук, доцент Департамента информационной безопасности Финансового университета при Правительстве Российской Федерации, г. Москва, Российская Федерация.*
E-mail: iasavelyev@fa.ru

[2] ***Боровская Ольга Евгеньевна,*** *магистрант Финансового университета при Правительстве Российской Федерации, г. Москва, Российская Федерация.*
E-mail: borovskaya_olechka@mail.ru

Типы облаков и облачных сервисов

Облака чаще всего подразделяют на три категории [6]:

- *частное* облако — облако, обслуживающее собственные потребности организации-владельца и полностью ею контролируемое;
- *публичное* облако — облако, предоставляющее свои сервисы широкому кругу пользователей (потребителей) для реализации их целей и контролируемое облачным провайдером;
- *гибридное* облако — комбинация публичного и частного облаков; через единую платформу позволяет работать с сервисами частного и публичного облаков.

Концептуально типы облаков на практике выглядят следующим образом.

При использовании *частного* облака «поверх» собственной виртуальной инфраструктуры появляется слой платформы частного облака. Данная платформа включает два основных компонента: платформа автоматизации (автоматизирует предоставление вычислительных ресурсов в виде преднастроенных сервисов: виртуальные машины, объектные хранилища, управляемые базы данных и др., т. е. автоматизирует взаимодействие с виртуальной инфраструктурой и автоматически разворачивает те или иные сервисы) и портал самообслуживания (обеспечивает взаимодействие пользователей с облаком: заказ сервисов, настройка, остановка и др.). При этом пользователи подключаются к порталу самообслуживания, выбирают интересующий их сервис, например, виртуальную машину, и заказывают его. Далее эта информация передается в платформу автоматизации, которая отдает команду гипервизору и разворачивает соответствующие сервисы в инфраструктуре (комплексе оборудования и средств виртуализации, вычислительные ресурсы которого предоставляются пользователям в виде сервисов), исходя из заранее заложенной логики.

При использовании *публичного* облака логика остается примерно той же самой, только теперь за нее отвечает третья организация. Облачный провайдер строит у себя облачную инфраструктуру — публичное облако — и предоставляет услуги (портал самообслуживания) своим клиентам. Для компаний, использующих публичное облако, это выглядит следующим образом: сервисы, развернутые в публичном облаке, взаимодействуют с периметром компаний через соединение *VPN* (*Virtual Private Network*), идущее «поверх» сети Интернет, либо через выделенный канал, что является более дорогостоящим решением.

При использовании *гибридного* облака в периметре компании разворачивается платформа гибридного облака, способная использоваться для организаций частного облака и взаимодействовать с собственной инфраструктурой, а также подключаться к публичным облакам. Для компаний, использующих гибридное облако, это выглядит следующим образом: через единый портал компании могут заказывать сервисы как в собственной инфраструктуре, так и в инфраструктуре публичного облака.

Типы облачных *сервисов*, разворачивающихся в этих облаках, также делятся на три категории.

Инфраструктурные сервисы (*IaaS — Infrastructure as a Service*) — традиционные элементы инфраструктуры, такие, как виртуальные машины с *OS Ubuntu*, разворачиваемые в облаке. Данные сервисы предоставляют элементы инфраструктуры *информационных технологий* (ИТ), доступные из сети Интернет. Известными провайдерами являются *DigitalOcean* и *AWS*.

Платформенные сервисы (*PaaS — Platform as a Service*) — сервисы, при которых облако предоставляет уже готовые технологические стеки, доступные из сети Интернет, такие как управляемые базы данных, когда за облачным провайдером стоит поддержка операционной системы и обеспечение доступности базы данных, а за пользователем остается только администрирование и веб-приложения. Известными провайдерами являются *Heroku* и *Azure*.

Сервисы *программного обеспечения* (ПО) (*SaaS — Software as a Service*) — сервисы, в которых для пользователей предоставляется уже преднастроенное ПО, доступное из сети Интернет по подписке. Примером такого сервиса может выступать онлайн-чат для общения среди работников. Известными провайдерами являются *Slack* и *Office* 365 [1].

При этом частные облака чаще всего предоставляют инфраструктурные и платформенные сервисы (*IaaS, PaaS*): *Openstack*, *ManageIQ*, *Morpheus* [4]. Публичные облака делятся на две категории:

– облака, предоставляющие инфраструктурные и платформенные сервисы (*IaaS, PaaS*): *AWS*, Яндекс Облако, *Azure*;
– облака, предоставляющие ПО-сервисы (*SaaS*): *Office* 365, *SalesForce*, *Zoom* и др.

Угрозы в облаке и разделение ответственности

Среди наиболее актуальных угроз, встречающихся как в частном, так и публичном облаке, выделяются следующие:

- недостаточный уровень информационной безопасности (ИБ) провайдера;
- неконтролируемый доступ к облачным сервисам [2];
- перехват контроля над ресурсами в облаке;
- несанкционированный доступ к *Application programming interface* (*API*);
- утечка конфиденциальных данных из облака;
- использование «теневых ИТ»[4].

[4] То есть не санкционированных ИТ-отделом компании оборудования, ПО и облачных сервисов. См.: Кораблев А. В., Петрушова М. В. Моделирование информационных рисков использования облачных технологий : учебное пособие. М. : Конверт, 2019. 164 с. ISBN 978-5-6043267-0-1.

В случае частных и публичных облаков появляется вопрос *разделения ответственности* (*табл.* 1) между провайдером и пользователем облачных сервисов. Эта таблица — концептуальная, т. е. в зависимости от облачного провайдера и конкретного сервиса, который будет использоваться в облаке, само разделение ответственности может меняться.

В случаях частного облака компания обеспечивает защиту на всех уровнях от физической инфраструктуры до уровня тех данных, которые обрабатываются в облачной платформе.

В случае публичного облака провайдер и пользователь берут на себя часть ответственности, организуя совместную работу. Таким образом, за клиентом остается меньший контроль, чем в собственной инфраструктуре. Это помогает сэкономить, но повышает важность контроля, остающегося на стороне клиента.

Таблица 1

Разделение обязанностей между провайдером и пользователем

Объекты	Частные облака	Публичные облака			Особенности
	IaaS/PaaS/SaaS	IaaS	PaaS	SaaS	
Данные	–	–	–	–	Повышение важности ИБ более высоких уровней (нет возможности компенсировать низкоуровневыми «контролями»)
Конечные устройства и пользователи	–		–	–	
Управление доступом	–	–	–	–	
Приложения	–	–	–	+	Передача провайдеру издержек на поддержание контроля; увеличение важности контрактов и соглашений об уровне сервиса
Сеть	–	–	+	+	
Хосты	–	–	+	+	
Физическая безопасность	–	+	+	+	
Обозначения:	– — ответственность пользователя + — ответственность провайдера облачных услуг				

Модель обеспечения информационной безопасности в облаке

Особенность защиты облаков вытекает из высокой степени автоматизации облачных платформ: повышается динамичность того ландшафта, который в облаке может быть развернут. Если раньше можно было обойтись ручными «контролями» (ручным администрированием и реализацией требований ИБ), то в настоящее время в облаке такие контроли не будут успевать за темпами облака. Для своевременного выявления и контроля всех изменений в инфраструктуре облака необходимо внедрять автоматизацию контроля ИБ и использовать уже готовые шаблоны.

Ранее основа безопасности облачных сред заключалась в защите сетевого периметра от внешних угроз. В связи с нынешней удаленной работой из-за пандемии грань сетевого периметра размывается. Сотрудники компаний, использующих облачные сервисы, выходят за пределы сетевого периметра при подключении к внутренним системам через незащищенные каналы связи, а также «потребляют» облачные приложения, которые подразумевают передачу каких-либо данных и процессов вне контролируемого сетевого периметра. Следовательно, в современной инфраструктуре защита *только* сетевого периметра недостаточна, что ведет к необходимости в обеспечении защиты на всех уровнях: сеть, приложения, доступ, данные.

В классической модели обеспечения ИБ контроль качества осуществляется перед внедрением системы [8]. В современной модели необходимо постоянно контролировать степень выполнения требований безопасности: анализировать качество и мониторить «здоровье» облачной системы.

Обеспечение ИБ в облаке — комплексная задача, которая достигается за счет комбинации «технологии — процессы» и включает следующие основные компоненты:

a) *классические подходы* (контроль доступа к облаку, защита от вредоносного ПО, защита периметра и др.);

b) *процессы* (процессы обеспечения ИБ для классической инфраструктуры: управление доступом, управление инцидентами, управление уязвимостями инфраструктуры, управление рисками — все это необходимо адаптировать к специфике облака, его инструментарию и модели разделения ответственности; уникальные процессы для современной инфраструктуры);

c) *облачные подходы* (индивидуальные подходы для уникальных облаков (использование встроенных инструментов обеспечения ИБ облака, шифрование данных в облаке, выбор облачного провайдера с учетом возможностей ИБ и др.) [5].

Продуктивный подход к защите облаков

Расширенное ви́дение защиты облаков основывается на лучших международных практиках, выработанных за более чем 10 лет существования облаков, а также на практике построения облачных платформ и миграции инфраструктуры из традиционного ландшафта в облака, защиты облачных сред. Данное ви́дение заключается в присоединении внешних сервисов (сервисов организаций-партнеров, государственных органов: платформ закупок, логистики и государственных сервисов) к классическому пониманию облака (частные, публичные).

Внешние сервисы схожи по своей организации с облачными приложениями, поскольку также контролируются сторонней организацией, а пользователям этих сервисов остается только правильно их использовать и контролировать их использование. Отличием внешних сервисов от облачных приложений организаций является то, что облачные приложения организаций самостоятельно определяют способ использования тех или иных приложений, а внешние сервисы реализуют жестко прописанную логику взаимодействия со сторонней организацией.

Тем не менее уровень контроля для облачных и внешних сервисов часто идентичен. Поэтому разумно расширять видение защиты облаков именно таким способом.

Центральная часть подхода — контроль ИБ, распределенный по 5 уровням, включая контроль, направленный на защиту: доступа, данных, приложений, инфраструктуры, а также на процессы обеспечения ИБ, адаптированные под облако. Каждый из этих уровней делится на 4 области применения (*табл.* 2):

- сами облака (частные и публичные облака) (расположены по центру таблицы);
- те стороны, которые взаимодействуют с облачной инфраструктурой (сотрудники компании и внешние взаимодействия) [11].

Таблица 2

Подход к защите облаков

<table>
<tr><th>Уровни</th><th>Работники</th><th>Частные облака</th><th>Публичные облака</th><th>Внешние взаимодействия</th></tr>
<tr><td rowspan="5">Доступ</td><td></td><td colspan="2">Разграничение зон ответственности в облаке*</td><td></td></tr>
<tr><td>Контроль сетевого доступа</td><td colspan="2">Контроль доступа к ресурсам</td><td></td></tr>
<tr><td rowspan="2">Контроль привилегированного доступа</td><td colspan="2">Управление секретами</td><td></td></tr>
<tr><td colspan="3">Интегрированное управление доступом*</td></tr>
<tr><td>Многофакторная аутентификация</td><td colspan="2">Управление доступом к API*</td><td></td></tr>
<tr><td rowspan="3">Данные</td><td rowspan="2">Управление правами на доступ к данным (IRM)*</td><td></td><td>Шифрование данных в облаке*</td><td rowspan="2">Виртуальные комнаты данных (VDR)</td></tr>
<tr><td colspan="2">Идентификация и классификация данных</td></tr>
<tr><td colspan="3">Защита от утечек данных</td><td></td></tr>
<tr><td colspan="4">Контроль передачи данных в облаке*</td></tr>
<tr><td rowspan="3">Приложения</td><td></td><td colspan="2">Защита web-приложений</td><td></td></tr>
<tr><td></td><td colspan="2">Защищенное взаимодействие сервисов в контейнерных средах*</td><td></td></tr>
<tr><td></td><td colspan="2" rowspan="2">Автоматизированные контроли ИБ в разработке / Безопасность контейнеров (DevSecOps)</td><td></td></tr>
<tr><td rowspan="5">Инфраструктура</td><td>Защита от вредоносного ПО</td><td></td></tr>
<tr><td>Управление мобильными устройствами</td><td>Защита платформы частного облака*</td><td>Оценка провайдера*</td><td></td></tr>
<tr><td>Контроль «теневых ИТ»</td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="2">Продвинутая защита рабочих станций</td><td>Защита инфраструктуры</td><td>Автоматизация политик безопасности</td><td></td></tr>
<tr><td colspan="2">Тестирование на проникновение и BAS</td><td></td></tr>
<tr><td>Интеграция с SOC</td><td colspan="2"></td><td></td></tr>
</table>

Процессы ИБ	Управление рисками ИБ	Тренинги и осведомленность	Политики и стандарты
	Анализ потоков данных, видение профилей пользователей	Регулярные требования	Управление инцидентами и проведение расследований
Обозначения и сокращения:	* — облачные подходы (остальные — классические подходы) API — Application programming interface IRM — Information Rights Management VDR — Virtual Data Room DevSecOps — Development, Security and Operations BAS — Breach and Attack Simulation SOC — Security Operation Center		

Многие компании, внедрив облачную инфраструктуру, уже сейчас сталкиваются с проблемой моментального внедрения *комплексного подхода* к защите облаков. Для этого были выделены 8 ключевых «контролей», которые необходимо выполнять для базовой защиты облака.

1. Идентификация используемых облаков: анализ сетевого трафика; использование ПО *Cloud Access Security Broker* (*CASB*).

2. Соответствие требованиям регуляторов: проверка надежности провайдера; реализация необходимых контролей для защиты ресурсов в облаке.

3. Защита доступа: усиленная аутентификация (*MFA — Multi-Factor Authentication*), доступ к доверенным устройствам; наименьшие достаточные привилегии.

4. Процессы ИБ в облаке: обновление процессов с учетом специфики облака.

5. Обучение работников: внутренние и внешние обучения; сдача сертификаций.

6. Настройка автоматизированных правил использования облака: ограничение доступных к использованию облачных сервисов; развертывание облачных ресурсов на основе шаблонов.

7. Автоматизация контролей ИБ в облаке: автоматическое выявление и блокировка несанкционированных изменений в облачных ресурсах.

8. Мониторинг ИБ: отправка событий из облака в *SIEM* (*Security Information and Event Management*).

Описание, способы и инструменты устранения основных угроз облачной инфраструктуры

1. Недостаточный уровень ИБ провайдера влечет за собой следующие угрозы обеспечения ИБ (ОИБ) облачной инфраструктуры:

a) угроза компрометации данных в облаке через уязвимую инфраструктуру провайдера;

b) угроза недоступности ресурсов и систем вследствие нарушения работы облачной платформы провайдера;

c) угроза невыполнения требований регуляторов;

d) необходимые действия для ОИБ — оценка провайдера и предоставляемых им облачных сервисов с учётом цели использования облака и «чувствительной» информации, которая будет обрабатываться в облаке [7]. Для ОИБ возможно использование методики *CSA* (*Cloud Security Alliance*). Применимые уровни фреймворка: инфраструктура.

2. Неконтролируемый доступ к облачным сервисам влечет за собой следующие угрозы ОИБ:

- доступ бывших сотрудников к внешним сервисам, используемым в компании (электронные торговые площадки, логистические системы, системы поиска субподрядчиков, облачные сервисы и др.);
- отсутствие контроля за используемыми внешними сервисами;
- отсутствие контроля за данными, передаваемыми во внешние сервисы;
- отсутствие контроля доступа к внешним сервисам;
- доступ с недоверенных и уязвимых устройств.

Необходимые действия для ОИБ следующие:

- выявление используемых облачных сервисов, анализ процессов их использования и критичности;
- разработка регламента контроля доступа пользователей к облачным сервисам, включающего комплекс организационных и технических мер;
- разработка ролевой модели и политик разграничения доступа к ресурсам;
- внедрение систем *PIM*/*PAM* (*Privileged Identity Management* / *Privileged Access Management*) для контроля действий администраторов;
- интеграция облака с *MDM*-системами (*Master Data Management*);
- тестирование на проникновение.

Для ОИБ возможен выбор следующих вендоров: *Indeed*, АйТи Бастион.

Применимые уровни фреймворка: доступ, данные.

3. Перехват контроля над ресурсами в облаке влечет за собой следующие угрозы ОИБ:

- сложность инвентаризации активов в облаке;
- отсутствие удобных инструментов контроля за вносимыми изменениями со стороны ИТ;
- отсутствие понимания процессов взаимодействия активов в облаке между собой и с внешним миром;
- сложность контроля процесса обновления и развертывания активов;

- отсутствие единой структурированной политики безопасности.

Необходимые действия для ОИБ следующие:

- обследование существующих активов и «жизненного цикла» ресурсов в облаке;
- разработка адаптированных под облако процессов;
- внедрение систем управления ИБ публичных облачных сред;
- внедрение систем контроля состояния облачных активов;
- создание экосистемы безопасности в частных облаках;
- разработка политик безопасности облачных активов [10].

Для ОИБ возможен выбор следующих вендоров: *Positive Technplogies*, АО «Лаборатория Касперского».

Применимые уровни фреймворка: доступ, инфраструктура, процессы ИБ.

4. Несанкционированный доступ к *API* влечет за собой следующие угрозы ОИБ:

- отсутствие разграничения и контроля доступа к *API*;
- внедрение вредоносного кода в запросы к *API*;
- эксплуатация уязвимостей функций аутентификации и авторизации *API*.

Необходимые действия для решения проблемы следующие:

- тестирование на проникновение;
- разработка требований к управлению доступом к *API*;
- настройка системы *API Gateway* для реализации политик доступа и ограничений на использование *API*;
- проектирование и внедрение системы *Web Application Firewall* (*WAF*) для контроля сетевых подключений к *API* сервисам.

Для ОИБ возможен выбор следующих вендоров: *Positive Technologies*, Код безопасности.

Применимые уровни фреймворка: доступ, приложения.

5. Утечка конфиденциальных данных из облака влечет за собой следующие угрозы ОИБ:

- сложность облачной инфраструктуры и инструментов управления приводит к ошибкам настройки механизмов разграничения доступа;
- слабый контроль информационных потоков на границе облака не позволяет выявить факт случайной публикации данных в облаке или умышленную утечку данных.

Необходимые действия для решения проблемы следующие:

- выявление критичных данных, хранящихся в облаке или перемещаемых туда;
- внедрение и настройка средств обнаружения и предотвращения неправомерных операций с конфиденциальными данными;
- настройка средств контроля доступа к данным;
- внедрение средств шифрования и токенизация данных в облаке.

Для ОИБ возможен выбор следующих вендоров: Код безопасности, *Positive Technologies*, *InfoWatch*, *SearchInform*.

Применимые уровни фреймворка: доступ, данные.

6. Использование «теневых ИТ» влечет за собой следующие угрозы ОИБ:

- отсутствие видимости относительно используемых облачных сервисов;
- отсутствие контроля за данными, передаваемыми в неконтролируемые облачные сервисы;
- отсутствие контроля за хранением данных в неконтролируемых облачных сервисах.

Необходимые действия для решения проблемы следующие:

- внедрение решений *CASB* для выявления используемых облачных сервисов и реализации политик контроля использования;
- внедрение решений *NGFW* (*Next-Generation Firewall*) для выявления и ограничения подключений к неконтролируемым облачным сервисам.

Для ОИБ возможен выбор следующих вендоров: Код безопасности, *Usergate*.

Применимые уровни фреймворка: инфраструктура.

Инструментарий соответствующих средств защиты облаков в настоящее время в России очень широк (*табл.* 3) [3].

Таблица 3

Инструменты обеспечения ИБ в облаке

Категории решений	Решаемые задачи	Инструменты
Облачные решения	Контроль используемых облачных приложений. Автоматизация контроля ИБ в облаке	CASB. Cloud Security Posture Management (CSPM)
Встроенные средства	Мониторинг и «журналирование» событий. Автоматизация контроля ИБ в облаке	AWS Cloud Watch / AWS Cloud Trail. Azure Policy
DevSecOps	Контроль зависимостей в коде. Анализ используемых образов	Static Application Security Testing (SAST) / Dynamic Application Security Testing (DAST). Configuration control (Chef InSpec)
Традиционные решения	Защита веб-приложений. Защита конечных устройств	WAF. Endpoint Detection and Response (EDR)

Заключение

Авторами проанализирован опыт работы инженеров по информационной безопасности, специализирующихся в области проектирования и внедрения средств защиты облачной инфраструктуры, что позволило

обосновать продуктивную типизацию и классификацию применяемых облаков,

определить наиболее актуальные угрозы, встречающиеся в частных и публичных облаках, и способы их устранения,

выделить особенности разделения ответственности между провайдером и пользователем облачных сервисов (*IaaS, PaaS, SaaS*),

а также обосновать продуктивный подход к обеспечению информационной безопасности в облаке.

Приведен перечень отечественных решений в области защиты облачной инфраструктуры.

Рецензент: ***Федосеев Сергей Витальевич,*** *кандидат технических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*
E-mail: fedsergvit@mail.ru

Литература

1. Алексеева Т.В., Миронов С.С. Способы хранения данных и виды облачных сервисов // Труды XIV Междунар. науч.-практ. конф. «Фундаментальная наука и технологии — перспективные разработки» (6—7 февраля 2018 г.). Т. 2. North Charleston (USA): CreateSpace, 2018. С. 77—81.
2. Винер В.Р., Диденко Д.В., Савинская Д.Н. Виды угроз в облачных сервисах сектора PaaS // Труды Междунар. науч.-практ. конф. «Роль науки в развитии социума: теоретические и практические аспекты (9—10 февраля 2018 г.). СПб. : Культ-Информ-Пресс, 2018. С. 31—32.
3. Геворкян С.М., Осока К.А. Организация защиты облачной инфраструктуры // Вектор экономики. 2019. № 6 (36). С. 97.
4. Клочек М.С., Парфенова А.С. Облачные технологии: виды и типы // Инновационное развитие. 2018. № 1 (18). С. 16—17.
5. Кочешков А.А., Сенькив Д.А. Информационная безопасность публичных облачных сервисов // Научно-технический вестник Поволжья. 2020. № 7. С. 70—72.
6. Кукунин Д.С., Маслова Е.А., Шумилов С.С. Облачные технологии. Достоинства и недостатки облачных технологий // Труды IX Междунар. науч.-техн. и науч.-метод. конф. «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2020) (26—27 февраля 2020 г.) / СПб. гос. ун-т телекоммуникаций им. проф. М.А. Бонч-Бруевича. В 4 т. Т. 2. СПб. : СПбГУТ, 2020. С. 451—455.
7. Ли Н.И., Русяева М.С., Богданова В.А. Снижение рисков информационной безопасности облачных сервисов // Молодежная научная школа кафедры «Защищенные системы связи». 2021. Т. 1. № 1 (3). С. 4—6.
8. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
9. Ловцов Д.А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005, 248 с. ISBN 5-02-033779-X.
10. Матвеев М.Д., Лукащик Е.П. Анализ механизмов безопасности облачных сервисов // Труды II Всеросс. науч.-практ. конф. «Прикладная математика: современные проблемы математики, информатики и моделирования» (22—25 апреля 2020 г.) / ФГБУ «РЭА» Минэнерго России. Краснодар : Краснодарский ЦНТИ — филиал ФГБУ «РЭА», 2020. С. 265—271.
11. Рыжов Д.И. Анализ методов оценки информационной безопасности при использовании облачных сервисов // Труды XXVII Междунар. науч.-техн. конф. студентов и аспирантов «Радиоэлектроника, электротехника и энергетика» (11—12 марта 2021 г.) / МЭИ. М. : Радуга, 2021. С. 193.

MODERN APPROACHES TO COMPLEX ENSURING OF CLOUD INFORMATION SECURITY

Ivan Savel'ev, *Ph.D. (Technology), Associate Professor at the Information Security Department of the Financial University under the Government of the Russian Federation, Moscow, Russian Federation.*
E-mail: iasavelyev@fa.ru

Ol'ga Borovskaia, *master's student at the Financial University under the Government of the Russian Federation, Moscow, Russian Federation.*
E-mail: borovskaya_olechka@mail.ru

Keywords: *information security, approaches, cloud, cloud protection, cloud technologies, cloud services, threats, provider, informatisation, software.*

Abstract

Purpose of the paper: justifying a productive approach to ensuring information security in cloud technologies.

Methods of study: system and expert analysis of cloud infrastructure protection mechanisms with a view to eliminate the main threats, classification of clouds used.

Study findings: approaches to cloud protection depending on the class of infrastructure used, i. e. private or public clouds, are described. Comparative analysis of division of responsibility between the provider and the user of such cloud services as IaaS, PaaS, SaaS is carried out, which shows that if a private cloud is used the company itself ensures protection at all cloud infrastructure levels but if a public cloud is used the company's protection control is more restricted which allows to save money on servicing personnel but renders it impossible to make significant modifications to the current infrastructure in order to comply with the requirements set by the regulatory authorities.

The practical importance of the study is confirmed by defining a set of practical recommendations for eliminating the main threats to cloud infrastructure by using information protection means of different categories, examples of which are presented in the paper.

References

1. Alekseeva T.V., Mironov S.S. Sposoby khraneniia dannykh i vidy oblachnykh servisov. Trudy XIV Mezhdunar. nauch.-prakt. konf. "Fundamental'naia nauka i tekhnologii – perspektivnye razrabotki" (6–7 fevralia 2018 g.), t. 2. North Charleston (USA): CreateSpace, 2018, pp. 77–81.
2. Viner V.R., Didenko D.V., Savinskaia D.N. Vidy ugroz v oblachnykh servisakh sektora PaaS. Trudy Mezhdunar. nauch.-prakt. konf. "Rol' nauki v razvitii sotsiuma: teoreticheskie i prakticheskie aspekty (9–10 fevralia 2018 g.). SPb. : Kul't-Inform-Press, 2018, pp. 31–32.
3. Gevorkian S.M., Osoka K.A. Organizatsiia zashchity oblachnoi infrastruktury. Vektor ekonomiki, 2019, No. 6 (36), p. 97.
4. Klochek M.S., Parfenova A.S. Oblachnye tekhnologii: vidy i tipy. Innovatsionnoe razvitie, 2018, No. 1 (18), pp. 16–17.
5. Kocheshkov A.A., Sen'kiv D.A. Informatsionnaia bezopasnost' publichnykh oblachnykh servisov. Nauchno-tekhnicheskii vestnik Povolzh'ia, 2020, No. 7, pp. 70–72.
6. Kukunin D.S., Maslova E.A., Shumilov S.S. Oblachnye tekhnologii. Dostoinstva i nedostatki oblachnykh tekhnologii. Trudy IX Mezhdunar. nauch.-tekhn. i nauch.-metod. konf. "Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii" (APINO-2020) (26–27 fevralia 2020 g.). SPb. gos. un-t telekommunikatsii im. prof. M.A. Bonch-Bruevicha. V 4 t., t. 2. SPb. : SPbGUT, 2020, pp. 451–455.
7. Li N.I., Rusiaeva M.S., Bogdanova V.A. Snizhenie riskov informatsionnoi bezopasnosti oblachnykh servisov. Molodezhnaia nauchnaia shkola kafedry "Zashchishchennye sistemy sviazi", 2021, t. 1, No. 1 (3), pp. 4–6.
8. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
9. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005, 248 pp. ISBN 5-02-033779-X.
10. Matveev M.D., Lukashchik E.P. Analiz mekhanizmov bezopasnosti oblachnykh servisov. Trudy II Vseross. nauch.-prakt. konf. "Prikladnaia matematika: sovremennye problemy matematiki, informatiki i modelirovaniia" (22–25 aprelia 2020 g.). FGBU "REA" Minenergo Rossii. Krasnodar : Krasnodarskii TsNTI – filial FGBU "REA", 2020, pp. 265–271.
11. Ryzhov D.I. Analiz metodov otsenki informatsionnoi bezopasnosti pri ispol'zovanii oblachnykh servisov. Trudy XXVII Mezhdunar. nauch.-tekhn. konf. studentov i aspirantov "Radioelektronika, elektrotekhnika i energetika" (11–12 marta 2021 g.). MEI. M. : Raduga, 2021, p. 193.