УДК 338

ОРГАНИЗАЦИЯ ЗАЩИТЫ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

Геворкян С.М.

к.э.н., доцент,

Кубанский государственный университет

Краснодар, Россия

Осока К.А.

Магистрант, 2 курс,

Кубанский государственный университет

Краснодар, Россия

Аннотация:

В статье рассмотрена организация облачной структуры предприятия и инструменты по её защите. Сформулированы рекомендации по совершенствованию безопасности облачной инфраструктуры.

Ключевые слова: облачная инфраструктура, средства защиты, инструменты информационной безопасности, нормативная база, облачные вычисления, многоуровневый подход системы защиты информации.

ORGANIZATION FOR THE PROTECTION OF THE CLOUD INFRASTRUCTURE

Gevorkyan S.M.

Associate Professor,

Kuban state University,

Krasnodar, Russia

Osoka K.A.
Magistrant, 2-nd year, faculty of economics,
Kuban State University
Krasnodar, Russia

Annotation:
The article considers the organization of the cloud structure of the enterprise. Tools to protect her. Recommendations for improving the security of cloud infrastructure are formulated.

Keywords: cloud infrastructure, security tools, information security tools, regulatory framework, cloud computing, multi-level approach of information security system.

Предприятия на сегодняшний день невозможно представить без информационных технологий. Современные компании нуждаются в обработке и получении информации простым способом, не затрачивая больших средств. Поэтому, упростить большинство бизнес-процессов – одна из основных задач предприятия.

Облачные технологии давно зарекомендовали себя в качестве неотъемлемой части структуры любой компании. Как показывают данные аналитической компании IDC (International Data Corporation) объём рынка облачных вычислений в 2018 году вырос на 19 % или 182,4 млрд. долларов. И по прогнозам на 2022 год должен вырасти до 331,2 млрд. долларов [4]. Это значит, что компании готовы вложиться в облачные вычисления. Но самым главным вопросом остаётся информационная безопасность.

Облачные технологии имеют ряд преимуществ, но имеет и риски. Любая компания с частным облаком имеет информационную безопасность на

традиционном уровне. В публичном же облаке, предприятие теряет контроль над личными данными и встают здесь главные вопросы: контроль данных, расположение публичного облака, гарантия безопасности и работоспособности.

Примеров по слитой информации клиентов компании предостаточно. Инцидент с компанией «Мегафон», когда каждому была доступна информация из личных смс-сообщений клиента или компания Google, где данные с облачного хранилища оказались в открытом доступе и любой желающий мог увидеть. Поэтому главным вопросом в организации облачной инфраструктуры компании всегда должен вставать информационная безопасность.

Для наглядности устройства облачной структуры рассмотрим схему строения многоуровневого подхода к системе защиты (рис.1). Это значит злоумышленнику добраться до данных придётся потратить очень много времени и сил т.к. придётся расшифровать ключ безопасности, даже если он его взломает спрограммированным вирусом, его ожидают ещё остальные 8 уровней, через которые он может быть заблокирован.

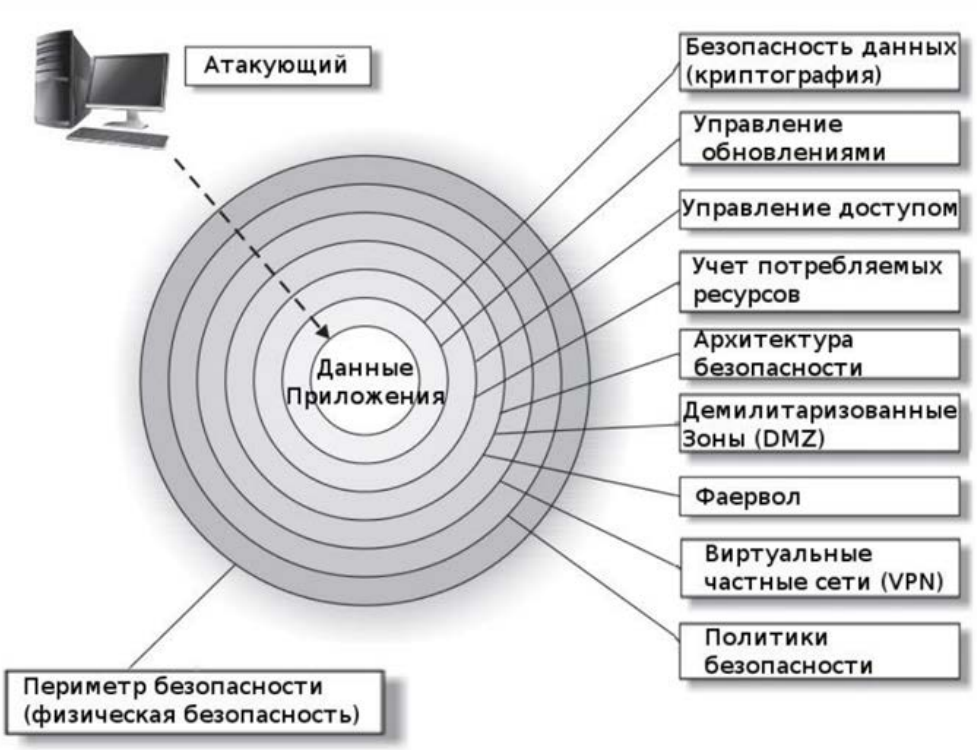

Рис.1 – Многоуровневый подход к системе защиты компьютерных систем.

Кратко охарактеризуем уровни защиты информации.

1. Безопасность данных (Криптография) – это шифрование канала данных, доступ к которым имеет только авторизованный пользователь или участник организации.

2. Управление обновлениями. Обновление подразумевает базу, в которой имеются компоненты защиты информации и поддержки ПО.

4. Учёт потребляемых ресурсов – это система, которая анализирует потребляемых ресурсов в данном случае виртуальной среды.

5. Архитектура безопасности – данный уровень является ничем иным как свойство, способное обеспечить целостность и секретность информации. Для конфиденциальности используются средства защиты информации от уничтожения или несанкционированного изменения.

6. DMZ (Демилитаризованная зона) – это сегмент сети, который отделяет

общедоступные сервисы от частных, то есть при запросе на внешнюю сеть, она должна отделить её от локальных ресурсов. Иными словами, dmz добавляет уровень безопасности сети.

7. Firewall – это такой барьер, который предотвращает доступ к нежелательным веб-хостингам. Иначе он выдаёт сообщение о том, что имеется угроза несанкционированного проникновения в компьютерную сеть.

8. Виртуальные частные сети (VPN) – Это совокупность сетевых соединений поверх другой сети интернет. Такие сети как правило дают безопасность путём их шифрования, и передача информации становится безопаснее.

9. Политика безопасности – это ряд принципов, правил, процедур в области безопасности, которые регулируют защиту информации.

Для решения вопросов безопасности информации, нужно проработать следующие направления:

– лицензирование деятельности поставщика услуг;

– аккредитация поставщика услуг;

– подходы к сертификации облачных решений;

– стандарты облачных решений;

– создание отличной инфраструктуры облачных решений;

– страховка рисков потребителей услуг.

Также стоит учесть все несанкционированные атаки на виртуальную инфраструктуру предприятия:

– несанкционированный доступ к системе виртуальной машины;

– перехват данных виртуальной инфраструктуры;

– захват ресурсов виртуальной инфраструктуры;

– использование уязвимости виртуальной инфраструктурой.

Так как у нас имеются три основные модели предоставления облачных услуг IaaS, SaaS, PaaS, которые имеют разные подходы и свою зону

ответственности поставщика и потребителя:

– управление данными;

– управление аутентификацией;

– соответствие требованиям информационной безопасности;

– обслуживание и конфигурация средств защиты информации;

– мониторинг информационной безопасности облачной структуры со стороны как поставщика так и потребителя услуг [2, 14].

Для управления информационной безопасностью имеются два подхода. Первый – совместный, второй – отдельный. Первый подход основан на нормативной базе ФСТЭК и ФСБ России, второй – на стандартах ISO/IEC 27001 и ISO/IEC 17799 (ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 17799-2005, которые регламентируют вопросы безопасности и рисков для информации [3,149].

При выборе провайдера нужно следовать следующим требованиям и рассмотреть ряд обязательств:

1. Провайдер должен в обязательном порядке сообщать клиентам об утечке информации, если таковой был.

2. Он не имеет права предоставлять информацию третьей стороне лиц или использовать для иных целей.

3. Если контракт компании с провайдером подошёл к концу, провайдер обязан удалить все данные клиента со своей облачной инфраструктуры.

4. Клиент должен знать местоположение облачного провайдера услуг.

5. Если клиент понёс потери информации в следствии халатности провайдера, провайдер облачных услуг должен возместить ущерб.

6. Каждый облачный провайдер должен иметь сертификацию и стандартизацию контрактов на использование облачных сервисов [1].

На сегодняшний день информационная безопасность облачных вычислений должна быть обеспечена средствами системы защиты

информации. Любая компания должна заботиться о том, куда передаётся информация, а также следить за состоянием программного и аппаратного обеспечения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ганька, Д. Облачные технологии в стандартах и законодательстве // Сетевые решения LAN. – 2016 - № 04 – Режим Доступа – URL: https://www.osp.ru/lan/2016/04/13049079/
2. Губарев, В., Савульчик, С., Чистяков, Н. Введение в облачные вычисления и технологии [Текст] / В. Губарев., С. Савульчик, Н. Чистяков – Нск.: НГТУ – 2013 – 14 с.
3. Шаньгин, В.Ф. Информационная безопасность и защита информации [Текст] / В.Ф. Шаньгин – М.: «ДМК-Пресс», 2017 – 149 с.
4. Облачные вычисления (мировой рынок) // Tadviser: Государство. Бизнес. IT 2019 – [Электронный ресурс] – Режим доступа – URL: https://vk.cc/9uARg4

Оригинальность 99%