Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

44. *Кравец В. В.* Доверенная вычислительная среда на планшетах Dell. «МАРШ!» //Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», 2014. Вып. 4 (107). С. 32-33.

45. *Счастный Д. Ю.* Ноутбук руководителя //Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19-21 мая 2015 г. – Минск: РИВШ, 2015. С. 112-113.

46. *Конявская С. В.* Про ДБО и планшеты //Национальный Банковский Журнал. М., 2014. № 10 (октябрь). С. 101.

ПАРАДИГМА БЕЗОПАСНОСТИ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В.А. АРТАМОНОВ

МНОО «Международная академия информационных технологий»

Технология «Облачные вычисления» появилась в информационной терминологии относительно недавно. Термин «Облачные вычисления» («Cloud Computing») начал применяться с конца 2007 - начала 2008 года, постепенно вытесняя понятие «Грид-вычисления» («Grid Computing»), фактически придя ему на смену. Одной из первых компаний, давших миру данный термин, стала компания IBM, развернувшая в начале 2008 года проект «Blue Cloud» и спонсировавшая Европейский проект «Joint Research Initiative for Cloud Computing». Метафорический образ «облако» уже давно используется специалистами в области сетевых технологий для изображения на сетевых диаграммах сложной вычислительной инфраструктуры (или же Интернета как такового), скрывающей свою внутреннюю организацию за определенным интерфейсом**.** Не задерживаясь на множестве определений, отражающих различные точки зрения и акценты авторов на эту информационную технологию (ИТ), остановимся на двух, которые отражают национальную стандартизацию данного понятия в общем контексте семантических отношений ИТ.

Национальный институт стандартов и технологий (НИСТ) США, 2011: *Облачные вычисления – информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру.*

Минкомсвязи РФ (опубликовано на Федеральном портале нормативных правовых актов), **2016**: *Облачные вычисления – информационные технологии, включающие в том числе государственную инфраструктуру облачных вычислений, обеспечивающие дистанционную обработку данных более чем одной информационной системой.* Отметим сразу, что это определение, достаточно радикальное и на наш взгляд вполне адекватное по сути, принципиальным образом отличается от общепринятого понимания облачных вычислений, под которыми подразумеваются не технологии, а модель взаимоотношений между поставщиком и потребителем ИТ.

Облачные вычисления обеспечивают практически неограниченную мощность, устраняя проблемы масштабируемости и открывают доступ к программным и аппаратным активам, которые большинство пользователей не могли бы себе позволить. В том числе, разработчики приложений, используя управляемые через Интернет облачные вы-

числения и активы, являющиеся результатом такой конфигурации, имеют доступ к ресурсам, позволяющим разрабатывать продукты ИТ, которые им были ранее не по плечу.

Контроль и управление облаками – является проблемой безопасности. Гарантий, что все ресурсы облака идентифицируемы и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака нет. Это высокоуровневый тип угроз, т.к. он связан с управляемостью облаком, как единой информационной системой и для него общую защиту нужно строить индивидуально. Для этого необходимо использовать модель управления рисками для облачных инфраструктур, которая должна предусматривать основную парадигму безопасности облачных технологий – *безопасность самого «облака» и безопасность внутри «облака»*.

В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. При переходе от физической инфраструктуры к виртуальной возникает множество новых угроз. При расширении виртуализации до облака их список расширяется, а возможный ущерб от их эксплуатации многократно возрастает. В отличии от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран (МЭ). Использование МЭ подразумевает работу фильтра, с целью разграничить внутренние сети облачного центра обработки данных (ЦОД) на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета или серверы из внутренних сетей. В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации. Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений.

Проблемы при перемещении физических серверов в вычислительное облако. Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных. Однако, виртуализация ЦОД и переход к облачным средам приводят к появлению новых угроз. Доступ через Интернет к управлению вычислительной мощностью один из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ персонала к серверам контролируется на физическом уровне, в облачных же средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

Динамичность виртуальных машин. Виртуальные машины динамичны. Создать новую машину, остановить ее работу, запустить заново можно сделать за короткое время. Они клонируются и могут быть перемещены между физическими серверами. Данная изменчивость трудно влияет на разработку целостности системы безопасности. Однако, уязвимости операционной системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени (например, при восстановлении из резервной копии). В средах облачных вычислениях важно надежно зафиксировать состояние защиты системы, при этом это не должно зависеть от ее состояния и местоположения.

Уязвимости внутри виртуальной среды. Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным ПО высока. Риск для виртуальных систем также высок.

Параллельные виртуальные машины увеличивает «атакуемую поверхность». Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

Защита бездействующих виртуальных машин. Когда виртуальная машина выключена, она подвергается опасности заражения. Доступа к хранилищу образов виртуальных машин через сеть достаточно.

На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение. В данном случаи должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

Защита периметра и разграничение сети. При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине.

Корпоративный МЭ – основной компонент для внедрения политики безопасности и разграничения сегментов сети, не в состоянии повлиять на серверы, размещенные в облачных средах.

Решения по защите от угроз безопасности

1. **Шифрование** – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в ЦОД, а также в случаи отсутствия необходимости, безвозвратно удалять.

2. **Защита данных при передаче**. Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случаи доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, IPsec давно используются провайдерами.

3. **Аутентификация** – защита паролем. Для обеспечения более высокой надежности, часто прибегают к таким средствам, как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой индетификациии при авторизации, также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

4. **Изоляция пользователей.** Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service).

По части предоставления услуг в «облаке» выделяют следующие основные сервисы:

программное обеспечение как сервис (SaaS) – обеспечивает аренду приложений. Потребители этих сервисов – конечные пользователи, они работают с приложениями в «облаке». Модель предоставления программного обеспечения как сервиса – модель обеспечения доступа к приложениям через Интернет с оплатой по факту их использования;

платформа как сервис (PaaS) – предоставляет возможность аренды платформы. Потребители – сами компании, разработавшие приложения. Платформа обеспечивает среду для выполнения приложений, сервисы по хранению данных и ряд дополнительных сервисов, например, интеграционные или коммуникационные;

инфраструктура как сервис (IaaS) – имеет возможность аренды серверов, устройства хранения данных и сетевого оборудования. Потребители – владельцы прило-

жений, ИТ-специалисты, подготавливающие образы ОС для их запуска в сервисной инфраструктуре. В этой модели могут быть запущены практически любые приложения, установленные на стандартные образы.

Теперь, исходя из выше изложенного, сформулируем некую исходную концептуальную схему, то есть **парадигму безопасности**, которая, в свою очередь, формирует модель злоумышленника и далее политику безопасности, которая должна найти отражение в нормативных документах на рассматриваемую технологию облачных вычислений. Предлагаемую парадигму изложим в виде некоторых постулатов, базирующихся на опыте реализации задач по созданию и обеспечению успешного функционирования конкретных систем информационной безопасности облачных вычислений, на анализе трудностей, о которых сказано ранее, на устранении противоречий, имеющихся в действующем подходе к решению этой весьма сложной проблемы, а главное – в получении эффекта, заметного для провайдера и пользователя и экономически ощутимого.

Далее в докладе рассматриваются постулаты безопасности, которые представляют собой кратко структурированные положения политики безопасности рассматриваемой информационной технологии.

СИСТЕМЫ МОНИТОРИНГА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.А. ДМИТРИЕВ, А.Б. СТЕПАНЯН, А.В. АФАНАСЬЕВ, Е.П. МАКСИМОВИЧ

Объединенный институт проблем информатики НАН Беларуси

В настоящее время все больше внимания уделяется обеспечению безопасности информации как в крупных учреждениях и компаниях, так и в средних и малых организациях. Защищаемые объекты имеют различные уровни доступа, всевозможные варианты развертывания вычислительных сред и разнообразные топологии сетевого взаимодействия.

Актуальной проблемой является проблема обнаружения и локализации вредоносной информации, находящейся внутри корпоративных сетей. Также растут количество и разнообразие информационных атак на ресурсы информационных систем.

Способы проникновения вредоносной информации в корпоративные информационные системы также стремительно модифицируются, что делает процесс нахождения вредоносной информации более трудоемким и требующим применения различных средств защиты информации.

В современных вычислительных сетях и информационных системах обычно используется большое количество разнородных средств защиты информации. Межсетевые экраны, системы обнаружения вторжений, сетевые устройства, операционные системы, антивирусы, базы данных, различные приложения генерируют огромное количество событий безопасности. Журналы событий каждого компонента хранятся отдельно, и вручную найти и сопоставить необходимую информацию для определения инцидентов информационной безопасности крайне сложно. Вместе с сигналами об активности злоумышленников от средств защиты информации поступает огромное количество ложных сигналов, что еще больше снижает эффективность работы сотрудников сетевой безопасности. При этом ответные действия на угрозы безопасности должны быть предприняты немедленно.