З.З. Ибрагимов, Н.А.Ибрагимова

Джизакский Политехнический Институт

Узбекистан. nargiza.anorovna.71@mail.ru

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ И МОБИЛЬНЫХ ЦИФРОВЫХ ПЛАТФОРМАХ

Контроль и управление облаками — является проблемой безопасности. Гарантий, что все ресурсы облака посчитаны 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 [11]. Для этого необходимо использовать модель управления рисками для облачных инфраструктур. 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 инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты [9]. 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 [7].

Мобильные устройства — неотъемлемая часть нашей жизни. Основные черты этого сегмента — повсеместная распространенность и быстрый количественный

рост [5]. По мере перехода компьютерной индустрии на мобильные платформы целью нападений все чаще становятся именно мобильные системы и приложения. Как показывает исследование компании Sophos , основной целью кибератак теперь является Android, а в отчете компании F-secure говорится, что за два предыдущих года число разновидностей зловредных мобильных программ увеличилось с нескольких сотен до более чем 50 тысяч. Всеобщая распространенность и популярность мобильных устройств приводит к чрезвычайной актуальности проблемы обеспечения безопасности мобильных приложений [3]. Поскольку в таких устройствах хранятся большие объемы личной информации, они являются привлекательными целями для атак злоумышленников, стремящихся к получению финансовой выгоды. Однако, по данным компании Symantec, только 57% взрослых пользователей знают о том, что существуют средства обеспечения безопасности мобильных объектов. Злоумышленников привлекает, с одной стороны, прямая связь устройства с реальными деньгами (мобильный банкинг, счет мобильного), которые несложно обналичить, а с другой — различная информация, которая может принести не меньший доход [4]. При личном использовании для защиты информации обычно обходятся ограничением доступа к устройству (пароль, PIN или графика для разблокировки) и приложением для поиска устройства в случае потери, реже устанавливают антивирус и шифрование данных флеш-памяти [1]. Для обеспечения безопасности мобильных платформ исследователи пытаются применять самые разные стратегии. В некоторых подходах в основном используются анализ, выявление и оценка зловредных приложений. Как и в традиционных подходах к обеспечению безопасности систем, анализ может опираться на использование статических и динамических методов или их комбинации. В корпоративной среде ситуация несколько иная. Зачастую на мобильном устройстве обрабатывается информация, не только составляющая коммерческую тайну, но и подлежащая обязательной защите в соответствии с законодательством РФ (например, персональные данные). Поэтому обязательным условием использования мобильного устройства для обращения к

служебной информации является защищенный удаленный доступ к сети, то есть доступ через VPN-клиент [2]. В зависимости от типа данных шифрование трафика может осуществляться по западным криптоалгоритмам или по отечественному ГОСТу. Активно применяются MDM-решения, осуществляющие контроль приложений, сетевых интерфейсов и многие другие параметры. Компания "Аладдин Р.Д." разработала смарт-карты и ридер для iPad/iPhone. Разработчики приложений для iOS могут использовать внешний сертифицированный криптографический модуль, который применяется в решениях для обеспечения безопасности. Это позволяет использовать усиленную квалифицированную электронную подпись на устройствах Apple.

Сегодня большинство производителей СКЗИ имеют в линейке своих продуктов клиенты безопасности для ОС Android [6]. Причем некоторые из них требуют получения административного доступа для установки (так называемое рутование), что, так же как и jail-break, является взломом ОС. Однако уже появились VPN-клиенты, не требующие прав администратора для установки, например, "С-Терра КлиентМ". Рассматривая рынок мобильных устройств, нельзя обойти вниманием еще одну ОС, на базе которой в последнее время появляется все больше смартфонов и планшетов. Это давно знакомая и привычная ОС Windows. Ситуация с защитой информации для устройств на платформе Windows 8 хорошо прогнозируема – о технологической совместимости своих продуктов с новой ОС уже заявили "Крип-тоПро", "С-Терра СиЭсПи", "Инфотекс", "Амикон" и другие. Данные решения пока не сертифицированы, но это вопрос времени, связанный с особенностями порядка сертификации [8]. Отметим, что использование внешне знакомой ОС, разработанной для хорошо известной x86-архитектуры, будет особенно удобно и приятно системным администраторам, и сотрудникам внутренней службы технической поддержки. Однако необходимо отметить, что между Windows 8 и мобильными версиями Windows существует некоторое различие. Если для Windows 8, как уже было сказано выше, вскоре появятся надежные, сертифицированные решения от известных производителей, то для мобильных

версий пока не анонсировалось ни одно решение для защищенного удаленного доступа. Кроме того, далеко не все привычные пользователям приложения портируются на мобильную ОС [11]. Таким образом, спокойным за безопасность своей информации пользователь может быть только при использовании ОС Windows версии до 7 и в самом скором времени – версии 8. Если же устройство работает на мобильной версии ОС Windows, то варианты VPN-защиты на рынке пока не предлагаются. Описанные решения по защите от угроз безопасности облачных вычислений неоднократно были применены системными интеграторами в проектах построения частных облаков. После применения данных решений количество случившихся инцидентов существенно снизилось. Но многие проблемы, связанные с защитой виртуализации до сих, требуют тщательного анализа и проработанного решения [10].

СПИСОК ЛИТЕРАТУРЫ

1. Бегматова, Н. З. (2020). Загрязнение и охрана окружающей среды. Причины и последствия. *Символ науки*, (6), 19-21.
2. Ibragimov, Z., & Ibragimova, N. (2021). Информационные технологии в сфере туризма в Узбекистане. *Boshlang'ich ta'limda innovatsiyalar*, *2*(2).
3. Ибрагимова, Н. А., & Ибрагимов, З. З. (2021). Платформа moodle–необходимый инструмент для преподователей. *Academic research in educational sciences*, *2*(CSPI conference 1), 572-575.
4. Ibragimov, Z. Z., & Ibragimova, N. A. (2022). Promising development of medical equipment technology.
5. Аллаберганова, Г. М., Кутбеддинов, А. К., Каримов, А. М., & Кудратов, Э. А. (2015). Интерактивные методы обучения студентов естественных специальностей на основании радиационных факторов экосистемы. *Педагогика и современность*, (1), 39-43.
6. Ziyatovich, I. Z., & Anorovna, I. N. (2022). The role of educational technologies in modern education.
7. Ibragimov, Z. Z., & Ibragimova, N. A. (2022). An iterative algorithm for constructing a delaunay triangulation.

8. Кузиева, С. У., & Имомова, Д. А. (2021). Защитные меры растения рода спирея. *Вопросы науки и образования*, (29 (154)), 10-13.
9. Искандарова, З. Преподавание и обучение с помощью информационно-коммуникационных технологий. *Экономика*, 912-918.
10. Бурлиев, А. У., & Рашидова, р. Методы обучения с использованием интерактивной и компьютерной технологий. *Uzacademia*, 43.
11. Ахмедов, А. А., Кудратов, Э. А., & Холов, Д. М. (2016). Инновационная технологии современных лабораторных работ по физике. *Инновационные технологии в науке и образовании* (pp. 228-230).