УДК 004.75 DOI: 10.17587/it.24.791-798

Р. Р. Фаткиева, канд. техн. наук, доц., e-mail: rikki2@yandex.ru,
С. Р. Рыжков, программист, e-mail: Ryzhkov@iias.spb.su,
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Оценка нарушения периметра информационной безопасности в облачной среде[1]

Рассмотрена задача оценивания безопасности виртуальной среды клиента, начиная с момента установления соединения и заканчивая получением результатов при использовании сервиса. Предложено использовать марковскую модель для выявления наиболее значимых угроз и прогнозирования состояния системы. Показано, что за счет применения комплекса мер по обеспечению информационной безопасности повышается не только вероятность успешной штатной работы, но и вероятность сбора дополнительных данных злоумышленником в связи с повышением интереса к системе.

Ключевые слова: *информационная безопасность, динамический периметр, облачная среда, информационные атаки*

Введение

Постепенная эволюция от замкнутых информационных сред с централизованной системой управления к формированию облачной среды с динамическим периметром и децентрализованным процессом управления приводит к тому, что для обеспечения информационной безопасности (ИБ) цифровых платформ недостаточно установки какого-либо одного средства защиты информации, поскольку имеет место их совместное использование. Важным условием для обеспечения ИБ цифровых платформ является реализация механизмов управления доступом. В работе [1] отмечается, что виртуальность облачных технологий привела к исчезновению традиционного физического периметра на основе контрольных точек, обеспечивавшего конфиденциальность информации. Периметр в цифровых платформах виртуализован, так как он определяется параметрами виртуальной среды и выполняемых приложений. На сегодняшний день существует актуальная проблема районирования и защиты географического ландшафта электронно-вычислительной структуры облачных вычислений при использовании цифровых платформ. Проблема обусловлена необходимостью:

- гарантированного доступа к отечественным и зарубежным информационным ресурсам [2];
- обеспечения безопасности и конфиденциальности миграции данных и приложений при использовании облачных вычислений в географически распределенных облачных хранилищах [3, 4];
- использования разнотипных вычислительных средств и систем, составляющих основу облачных вычислений, нередко разнородных и от разных производителей, что может повлечь за собой не только сбои в работе виртуальной среды, но и множество различных атак на нее [5, 6];
- понижения вероятности преодоления систем защиты при получении несанкционированного доступа к управлению виртуальной средой [7, 8];
- ограничения доступа физическим и юридическим лицам к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено;

[1] Работа выполнена при частичной поддержке гранта РФФИ 16-29-09482.

- атрибуции и отслеживания перемещения информации в целях создания матрицы доступа и контроля над уровнем предоставляемых прав [9—11].

Для определения общего числа возможных уязвимых мест (поверхностей атак) целесообразно классифицировать угрозы, систематизировать их в виде таксономии.

Таксономия как иерархическая система соподчиненных рангов безопасности облачных вычислений рассматривается в свете количественного анализа актуальных проблем безопасности для облачных вычислений, которые зависят от архитектуры. Базовая архитектурная классификация включает сети, хосты, приложения, данные (информацию об их безопасности и хранении), управление безопасностью, идентификацией и доступом — все эти элементы напрямую связаны с инфраструктурой и архитектурой реализации облачных решений.

Однако при использовании облачных вычислений периметр динамически изменяется, размывается за счет многоуровневой туннелированной вложенности и зависит от прохождения пакета по стеку протоколов. Каждый уровень вложенности позволяет создать снимок своего периметра, что позволяет, используя привязку к физическому периметру, затем разместить их на карте.

На рис. 1 отображены векторы атаки злоумышленника вне периметра провайдера облачных вычислений и внутри, в случае, когда злоумышленник получил доступ в качестве легитимного пользователя облачной инфраструктуры. Облачные вычисления позволяют отказаться от классической архитектуры, где в случае нарушения периметра вся защищаемая сеть находится под угрозой. Периметр безопасности, поставляемый как услуга, физически и логически отделен и изолирован от защищаемой сети. Физический периметр в системах контроля и управления доступом (СКУД) также оперирует понятием "граница" в контексте границы контролируемой зоны. В настоящее время известны модели, которые основываются на противоречиях между уровнем защищенности и доступности информационных ресурсов в пределах периметра [12—16]. Однако в описываемых моделях не учтена вероятность повышения интереса злоумышленника при обнаружении уровня защищенности, не соответствующего предполагаемой им ценности защищаемого информационного ресурса. Также на практике реализована методика, включающая в себя обоснование мероприятий обеспечения информационной безопасности в информационной системе [17, 18], в которой не охвачен вопрос использования облачных технологий, предоставляемых гарантированным поставщиком.

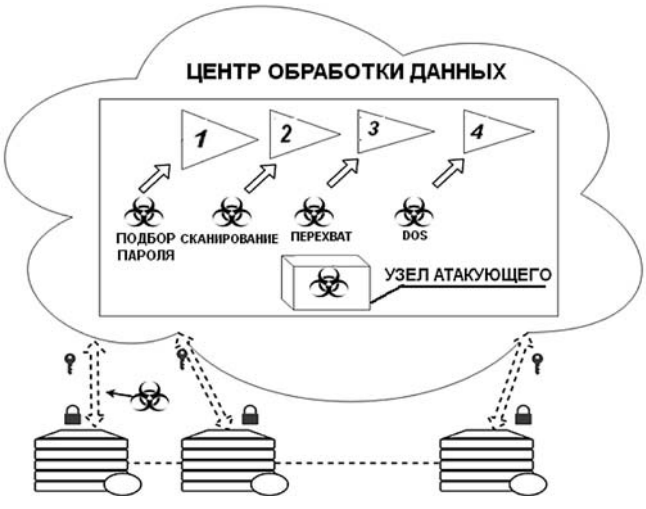


Рис. 1. Атаки на физический и облачный периметр

В работе [14] представлено комплексное решение для повышения уровня доверия в цифровых платформах, в основе этого решения — мандатный контроль доступа и надежные вычислительные технологии (измеряемая загрузка, аттестации и запечатывания). Такой подход создает гарантированную среду и явно связывает зашифрованные виртуальные машины с ранее аттестованными узлами, однако не представляет для оценки количественные значения.

Таким образом, важным условием для обеспечения безопасности информационной системы, построенной с использованием технологий облачных вычислений, является определение уязвимого для атаки места на всей поверхности защищаемого периметра исполняемых приложений в целях ее предотвращения. В статье рассматривается задача определения риска нарушения безопасности как внутри периметра облачных вычислений, так и "снаружи" миграции данных за счет перехвата трафика, а также подбора мероприятий для их снижения.

1. Постановка задачи

Рассмотрим постановку задачи на практическом примере доступа к облачному ресурсу. Ключевым вопросом при использовании облачной среды является безопасность виртуальной среды клиента, начиная с момента уста-

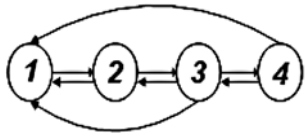


Рис. 2. Штатный процесс установления соединения

новления соединения и заканчивая получением результатов при использовании сервиса. В обобщенном виде процесс доступа к вычислительному ресурсу может быть представлен в виде графа состояний (рис. 2).

В частности, он соответствует процессу установления соединения по протоколу TCP/IP. Согласно графу (рис. 2) в процессе доступа могут быть выделены следующие состояния: *1* — клиент запускает исполняемый файл; *2* — осуществляется открытие сессии; *3* — передача данных по каналам связи; *4* — установление соединения.

Требуется разработать подход, позволяющий оценить риски нарушения безопасности в облачной среде, а также выработать мероприятия по противодействию представленным атакам.

Поскольку события описываемого операционного процесса дискретны, а время выполнения непрерывно, то сам процесс может быть представлен как процесс с отсутствием последействия, т. е. он обладает марковским свойством. В этом случае процесс перехода из состояния в состояние возможно описать системой дифференциальных уравнений, позволяющей учитывать не только вероятности наступления того или иного события, но влияние мероприятий по защите на процессы, происходящие в облачной среде.

2. Модель облачной среды в условиях информационных угроз

Определим показатель периметра защищенности облачных вычислений как вероятность того, что нарушение безопасности не произойдет. В этом случае защищенность облачных вычислений можно определить через математическое ожидание ущерба от нарушения защищаемых хостов $M_j = \sum_{i=0}^{N} \gamma_i P_{ij}(t)$, где $P_{ij}(t)$ — вероятность нарушения безопасности i-го хоста в момент времени t при j-м методе защиты; $i = \overline{1, N}$ — число представленных в системе виртуальных хостов; $j = \overline{1, K}$ — число возможных вариантов защиты; γ_i — значение ущерба от нарушения безопасности i-го хоста. Выполнение оценки возможно при условии, что атаки являются независимыми, а работа виртуальных хостов не коррелируется.

Для нахождения $P_{ij}(t)$ на каждом i-м виртуальном хосте определим методику, включающую следующие шаги:

Шаг 1. Определение процессов S_i, происходящих в системе, в штатном режиме функционирования.

Шаг 2. Формирование перечня атак $A_i(t)$ и построение модели угроз в облачной среде.

Шаг 3. Определение интенсивностей λ_i перехода процесса S_i из состояния в состояние и нахождение начальных состояний на момент $t = 0$.

Шаг 4. Решение системы дифференциальных уравнений относительно полученных интенсивностей перехода и начальных состояний.

Шаг 5. Получение значений вероятностей $P_{igr}(t)$ перехода из состояния q в состояние r на основе рассмотренной ранее системы дифференциальных уравнений для различных наборов значений интенсивностей, характерных для альтернативных мероприятий защиты.

Шаг 6. Влияние на процесс функционирования системы. Определение наилучшего варианта мероприятий по обеспечению информационной безопасности защиты согласно

$$M_j = \min_{\lambda \in \Omega} \sum_{i=0}^{N} \gamma_i P_{ij}(t).$$

Для построения простейшей модели расширим процесс доступа к вычислительному ресурсу (рис. 3) с учетом возможных угроз. В этом варианте процесса можно выделить следующие состояния: *1* — запуск программы; *2* — открытие сессии; *3* — передача данных по каналам связи; *4* — установление соединения с сервером; *5* — процесс аутентификации; *6* — про-

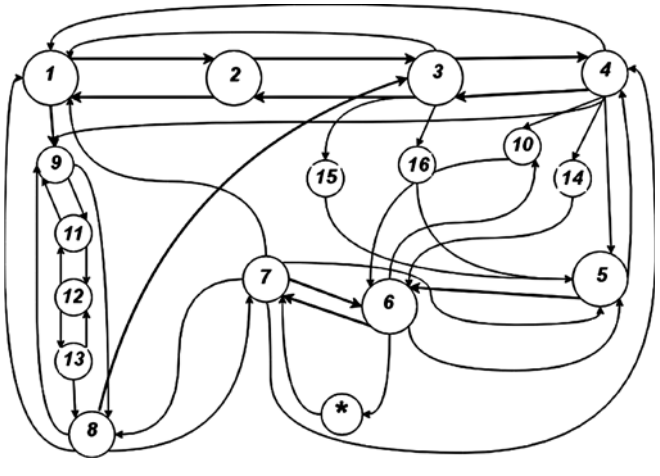


Рис. 3. Процесс доступа к вычислительному ресурсу при нарушениях ИБ

цесс авторизации; *7* — атака, направленная на подбор пароля; *8* — процесс получения доступа к управляемому ресурсу; *9* — атака, направленная на анализ приложения; *10* — атака Ddos; *11* — атака, направленная на сканирование порта; *12* — процесс получения данных о порте; *13* — процесс получения доступа к ОС; *14* — внедрение произвольного кода в SQL-запрос; *15* — процесс перехвата трафика; *16* — атака, направленная на подмену маршрутизатора; * — подделка (компрометация) криптоключа.

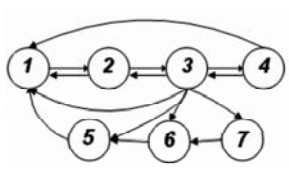
Оценка процессов, происходящих при доступе к сервису, позволяет выделить четыре основных этапа, которые необходимо осуществить для получения доступа к ресурсу: установление соединения, аутентификация, авторизация, доступ к ресурсу. Каждый из этапов представляет собой последовательный набор действий, приводящий к результату, но затрудняющий работу пользователя при осуществлении атаки. В связи с этим целесообразно рассмотреть частные модели возможных угроз на каждом из этапов.

3. Результаты моделирования

Моделирование нарушения установления соединения. В отличие от стандартного исполняемого файла, содержащего программу в виде, в котором она может быть исполнена компьютером, среда исполнения, а следовательно, и периметр исполняемого приложения, располагается не только на локальном вычислительном устройстве, но и в облаке. Перед исполнением программа загружается в память, и выполняются некоторые подготовительные операции (настройка окружения, загрузка библиотек), необходимые для связи с распределенными вычислительными ресурсами. Далее осуществляется открытие сессии и установление соединения. Для построения модели угроз и оценки состояния нарушения осуществим моделирование процесса получения доступа с возможными нарушениями:

- *атака, направленная на подбор пароля:* атака, в основе которой лежит метод перебора по словарю. С точки зрения теории вероятностей выбор пароля детерминирован и закономерен. В качестве пароля могут выступать: дата рождения, имя, предмет, набор цифр, последовательность близко расположенных на клавиатуре букв. В общем случае происходит конкатенация вышеперечисленного, поэтому предопределенность в выборе пароля играет ключевую роль в выборе алгоритмов, на которых основан метод перебора по словарю. Алфавитный пароль, сгенерированный человеком, неравномерно распределен в пространстве алфавитных последовательностей. Данное условие может быть учтено с большой точностью в марковских фильтрах нулевого и первого порядка (*нулевой порядок модели Маркова*: каждый символ генерируется в соответствии со своим вероятностным распределением и независимо от предыдущих символов; *первый порядок модели Маркова*: каждой диаграмме (упорядоченной паре) символов присваивается вероятность и каждый символ порождается в условной зависимости от предыдущего);
- *атака, направленная на перехват сетевых пакетов:* поскольку при передаче данных создается непрерывный динамический канал, проходящий через отдельные сегменты сети, создается возможность прослушивания и перехвата сетевых пакетов;
- *атака, направленная на навязывание ложного маршрутизатора:* атака канального или сетевого уровня, приводящая к перенаправлению сетевых пакетов жертвы или всего трафика сегмента на ненадлежащий адрес или к отказу в обслуживании (no route to host). Для защиты от ложного маршрута и подмены сервера применим технологию DNS поверх TLS. Целью данного метода является повышение конфиденциальности и безопасности пользователей путем предотвращения перехвата и манипулирования данными DNS.

Для представленных атак граф перехода из состояния в состояние и соответствующая система дифференциальных уравнений представлены на рис. 4, *а*, *б*.



а)

$$\begin{cases} \frac{dP_1(t)}{dt} = \lambda_{41}P_4 + \lambda_{31}P_3 + \lambda_{21}P_2 + \lambda_{51}P_5 - \lambda_{12}P_1 \\ \frac{dP_{21}(t)}{dt} = \lambda_{12}P_1 + \lambda_{32}P_3 - (\lambda_{23} + \lambda_{21})P_2 \\ \frac{dP_3(t)}{dt} = \lambda_{23}P_2 + \lambda_{43}P_4 - (\lambda_{32} + \lambda_{34} + \lambda_{35} + \lambda_{36} + \lambda_{37})P_3 \\ \frac{dP_4(t)}{dt} = \lambda_{34}P_3 - (\lambda_{41} + \lambda_{43})P_4 \\ \frac{dP_5(t)}{dt} = \lambda_{35}P_3 + \lambda_{65}P_6 - \lambda_{51}P_5 \\ \frac{dP_6(t)}{dt} = \lambda_{36}P_3 + \lambda_{76}P_7 - \lambda_{65}P_6 \\ \frac{dP_7(t)}{dt} = \lambda_{37}P_3 - \lambda_{76}P_7 \end{cases}$$

б)

Рис. 4. Граф перехода из состояния в состояние и соответствующая система дифференциальных уравнений:

а — штатный процесс установления соединения; *б* — система дифференциальных уравнений

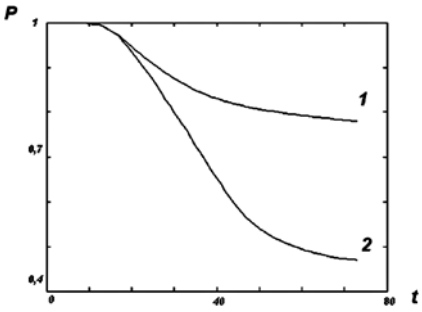


Рис. 5. Вероятность запуска программы

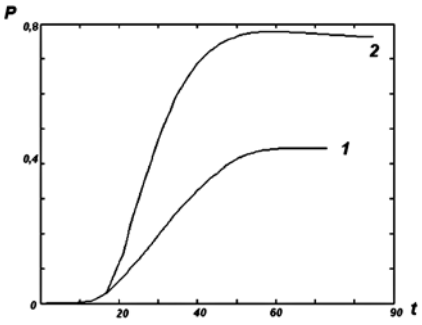


Рис. 6. Вероятность открытия сессии

В момент запуска программы (рис. 5, кривая *1*) вероятность приближена к единице и с течением времени снижается (согласно проблеме останова) до состояния, когда можно утверждать, что программа зависла. Критическая точка процесса определена 20-й секундой. На рис. 5 представлен график кривой *2*, полученный с использованием моделирования мероприятий по повышению вероятности успешного запуска (использование "песочницы", т. е. изолированной среды исполнения, антивирусной защиты, контроля целостности приложений и разделение прав доступа пользователей). Это позволяет оценить влияние введения тех или иных мер по защите на протекание процесса.

Зависимость процесса открытия сессии от процесса запуска программы. Вероятность открытия сессии обеспечивается запуском программы (рис. 6, кривая *1*), созданием нового соединения, инициируемого исполняемым файлом, с передачей пакета. Будем считать, что одновременно с созданием сессии открывается порт TCP/IP для последующей передачи данных и установления соединения с распределенными вычислительными ресурсами. Такая последовательность действий обеспечивает рост вероятности до определенного момента, на которую могут повлиять атаки: MITM, DDOS. Для обеспечения успешного открытия сессии, а также в целях противодействия нарушениям безопасности и в качестве мер повышения вероятности было предложено шифрование сетевого трафика на канальном уровне (аппаратный VPN "точка-точка" с криптографическим модулем). Анализ результатов моделирования показал эффективность проведенных мероприятий по защите (рис. 6, кривая *2*).

Вероятность успешной передачи данных по каналам связи. Как и на предыдущем графике, прослеживается зависимость процесса передачи данных по каналам связи от процессов, его образующих (рис. 7, кривая *1*). Критической точкой жизнеспособности процесса является тот же момент, при котором в процессе запуска приложения появляются те или иные проблемы с загрузкой. На рис. 7 представлен график кривой *2*, полученный после моделирования мер по повышению вероятности успешной передачи данных с использованием туннелирования в каналах передачи данных (VPN-канал). Моделирование показало, что влияние туннелирования на процесс передачи не существенно, однако вероятность передачи повышается.

Результаты оценки вероятности того, что в данный момент происходит установление соединения с сервером, аналогичны предыдущему процессу (рис. 8, кривая *1*). На рис. 8 (кривая *2*) изображена вероятность успешного установления соединения с сервером при противодействии нарушению безопасности. Были реализованы следующие меры: ограничение доступа по геолокации (GeoIP Block), динамическая блокировка IP-адресов "разрешенных стран" согласно правилам фильтрации пакета, установлен VPN-канал.

Вероятность атаки, направленной на подбор пароля, моделируется в момент соединения программы с сервером (рис 9, кривая *1*). С точки зрения теории вероятности выбор пароля детерминирован, поэтому применение генераторов паролей с аппаратным датчиком случайных чисел снижает вероятность успешной атаки (рис. 9, кривая *2*).

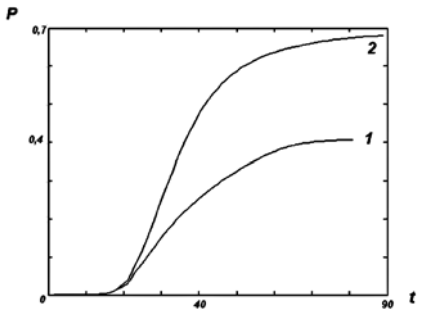


Рис. 7. Вероятность успешной передачи данных по каналам связи

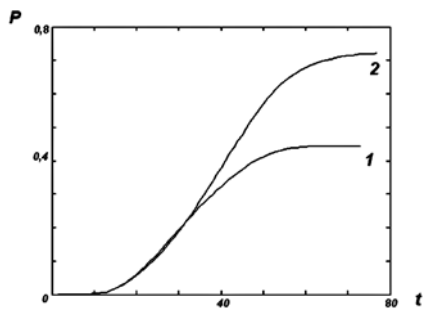


Рис. 8 Вероятность установления соединения с сервером

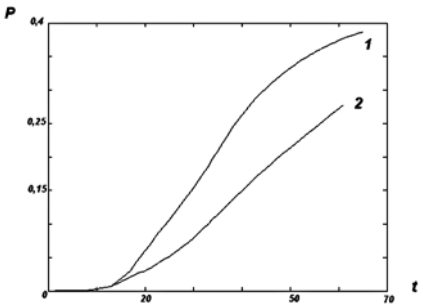


Рис. 9 Вероятность успешной атаки подбора пароля

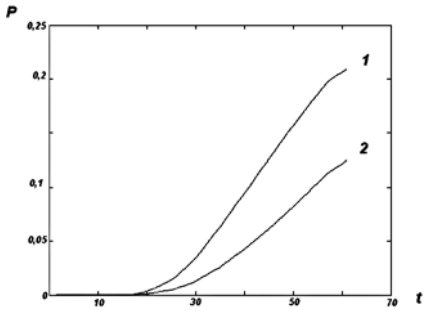


Рис. 10. Вероятность успешного перехвата сетевых пакетов

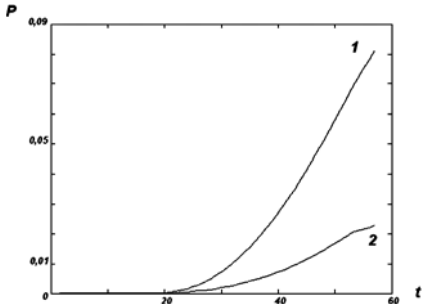


Рис. 11. Вероятность успешного навязывания ложной маршрутизации пакетов

Вероятность успешного перехвата сетевых пакетов в целях их дальнейшего анализа растет на временном интервале (рис. 10, кривая *1*) и связана с установлением соединения между приложением и сервером. Рис. 10 (кривая *2*) демонстрирует, что процесс обнаружения атак (процесс оценки подозрительных действий узлов сети) понижает вероятность перехвата.

Атака канального или сетевого уровня приводит (рис. 11, кривая *1*) к перенаправлению сетевых пакетов жертвы или всего трафика сегмента на ненадлежащий адрес или к отказу в обслуживании (no route to host). Вероятность атаки зависит от успешности соединения с сервером, повышается по мере его установления. Результаты моделирования противодействия навязывания ложной маршрутизации пакетов с применением фильтрации проходящих ICMP-сообщений Redirect понижает вероятность атаки почти вдвое (рис. 11, кривая *2*).

Полученные результаты моделирования с учетом всей совокупности введенных мероприятий по защите (в таблице и на рис. 12) позволяют определить влияние мер по обеспечению безопасности на уязвимые элементы в анализируемых процессах. Полученные решения применимы при планировании мероприятий по защите критически важных объектов от рассматриваемых угроз с учетом количественной оценки вероятности нарушения. Использование данной методики позволяет оценить целесообразность мероприятий обеспечения безопасности в анализируемом объекте.

Целесообразность таких мероприятий определяется достижением максимальной защиты при минимальных затратах и характеризуется следующими факторами: масштабностью и ресурсоемкостью сети, необходимостью применения однотипных технологий и средств защиты информации при проведении мероприятий по обеспечению системы защиты информации.

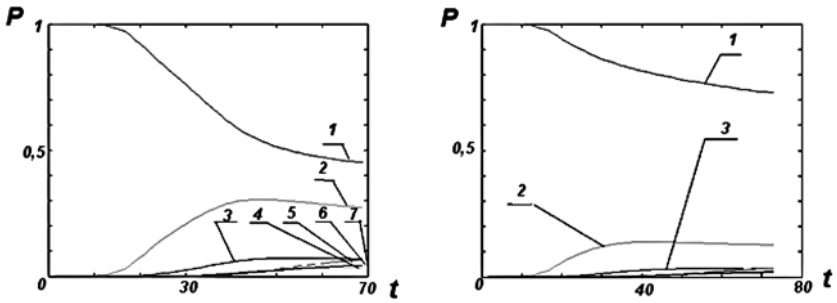


Рис. 12. Оценка вероятности нарушения безопасности:
а — без мер защиты; *б* — с учетом всей совокупности введенных мероприятий по защите

Оценка вероятности нарушения безопасности

Процесс	Вероятность без мероприятий по обеспечению безопасности	Вероятность при мероприятиях по обеспечению безопасности
Запуск программы (кривая *1* на рис. 12)	0,47	0,77
Открытие сессии (кривая *2* на рис. 12)	0,3	0,7
Передача данных (кривая *3* на рис. 12)	0,07	0,5
Соединение с сервером (кривая *4* на рис. 12)	0,07	0,6
Атака, направленная на подбор пароля (кривая *5* на рис. 12)	0,03	0,18
Атака, направленная на перехват сетевых пакетов (кривая *6* на рис. 12)	0,03	0,09
Атака, направленная на навязывание ложного маршрутизатора (кривая *7* на рис. 12)	0,03	0,04

Заключение

Анализ полученных в ходе исследования результатов моделирования процессов безопасности виртуальной среды клиента и применения комплексного подхода к обеспечению информационной безопасности показал следующее. Современные стереотипы по защите процессов клиентов виртуальной среды не в полной мере готовы противостоять текущим угрозам и новым вызовам безопасности. В связи с этим возникает необходимость совершенствования научно-методического аппарата. На примере конкретной задачи с типовыми процессами использована марковская модель для выявления наиболее значимых угроз, целесообразных мероприятий защиты и прогнозирования состояния системы. Аналогичная методика может быть использована для других моделей безопасности, для нахождения целесообразных мероприятий защиты и прогнозирования состояния системы. Применение полученных результатов в процессе построения, эксплуатации и модернизации системы информационной безопасности, предоставляющей облачные услуги, ведет к повышению эффективности и качества обслуживания и позволяет эффективно управлять процессом информационной безопасности.

Список литературы

1. **Analysis** of Cloud related Security and risks mitigation IRACST // International Journal of Advances Computing, Engineering and Applications (IJACEA). 2012. Vol. 1, N. 2. P. 40—49, 2012.

2. **Гюнтер Е. С., Нарутта Н. Н., Шахов В. Г.** "Облачные" вычисления и проблемы их безопасности // Омский научный вестник. 2013. № 2 (120). С. 279—282.

3. **Саклаков В. М.** Облачные вычисления: современные модели предоставления услуг и возможные риски // Молодежь и современные информационные технологии: сб. тр. XIII Междунар. науч.-практ. Конф. студентов, аспирантов и молодых ученых, г. Томск, 9—13 ноября 2015 г. Томск: Издво ТПУ, 2016. Т. 2. С. 104—106.

4. **Фролов Д. Б., Грунюшкина С. А. Старостин А. В.** Информационная геополитика и сеть Интернет. М.: РФК-Имидж Лаб, 2008. 404 с.

5. **Юсупов Р. М., Шишкин В. М.** О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. 2008. № 6. С. 11—23.

6. **Петров Д. Л.** Оптимальный алгоритм миграции данных в масштабируемых облачных хранилищах // Управление большими системами: сб. тр. 2010. № 30. С. 180—197.

7. **Воробьев В. И., Рыжков С. Р., Фаткиева Р. Р.** Защита периметра облачных вычислений // Программные системы: теория и приложения. 2015. Т. 6, № 1 (24). С. 61—71.

8. **Коваленко О. С.** Обзор состояний, проблем и перспектив хранения и анализа данных в "облаке" // Информатика, вычислительная техника и инженерное образование. 2011. № 5. С. 39—49.

9. **Каменщиков А. А.** Облачные технологии и интероперабельность информационных систем в здравоохранении // Журнал радиоэлектроники: электронный журнал. 2013. № 2. URL: http://j re.cplire.ru/j re/feb 13/11/text.pdf. (дата обращения: 28.06.l8).

10. **Чемеркин Ю. С.** Облачные вычисления как инструмент обработки конфиденциальной информации // Вестник РГГУ. Сер.: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2012. № 14. С. 53—65.

11. **Mauw S., Verschuren J. H. S., de Vink E. P.** A formalization of anonymity and onion routing // Computer Security—ESORICS 2004. Springer Berlin Heidelberg, 2004. C. 109—124.

12. **Gupta S., Kumar P.** Taxonomy of cloud security // International Journal of Computer Science, Engineering and Applications (IJCSEA). October 2013. Vol. 3, N. 5, P. 47—67.

13. **Lonea A. M., Popescu D. E., Tianfield H.** Detecting DDoS attacks in cloud computing environment // International Journal of Computers Communications & Control. 2013. Vol. 8. P. 70—78.

14. **Simma A.** Trusting Your Cloud Provider: Protecting Private Virtual Machines // Magdeburger Journal zur Sicherheitsforschung, Vol. 1. P. 530—539. Retrieved June 17, 2015, URL: http://www. sicherheitsforschung-magdeburg. de/publikationen. html (Version 2015/06/16 20: 01).

15. **Pivoting** in Amazon Clouds URL: http://andresriancho. github.io/nimbostratus/pivoting-in-amazon-clouds.pdf html (Version 2013/10/27 20: 48).

16. **Adrian D. et al.** Imperfect forward secrecy: How Diffie-Hellman fails in practice // Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015. P. 5—17.

17. **Осипов В. Ю., Носаль И. А.** Обоснование мероприятий обеспечения информационной безопасности // Информационно-управляющие системы. 2013. № 2 (63). С. 48—53.

18. **Осипов В. Ю., Носаль И. А.** Обоснование периода пересмотра мероприятий по защите информации // Информационно-управляющие системы. 2014. № 1. С. 63—69.

19. **Потапов В. И.** Постановка и решение игровой задачи противоборства аппаратно-избыточной динамической системы с атакующим противником, действующим в условиях неполной информации в процессе конфликта // Мехатроника, автоматизация, управление. 2017. Т. 18, № 8. С. 525—531.

R. R. Fatkieva, Senior Researcher, e-mail: rikki2@yandex.ru,
R. R. Ryzhkov, Engineer, e-mail: Ryzhkov@iias.spb.su,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
199178, St. Petersburg, Russian Federation

Assessment of Violations of Information Security Perimeter in the Cloud

The processes influencing the safety of the virtual environment of the client, from the moment of establishing the connection till obtaining the results, were investigated. It is proposed to use the Markov model to identify the most significant threats and to predict the state of the system. It is shown that due to the information security, not only the probability of successful regular workload is increased, but also the probability of collecting additional data by an intruder due to increased interest in the system. The analysis of the results of modeling the processes of security of the virtual environment of the client and the application of an integrated approach to ensuring information security, showed the following. Modern stereotypes to protect the processes of virtual environment are not fully ready to withstand current threats and new security challenges. In this regard, there is a strong need to improve the scientific and methodological apparatus. Using the example of a specific task with typical processes, the Markov model was used to identify the most significant threats, expedient measures for protecting and predicting the state of the system. A similar methodology can be used for other security models, for finding appropriate protection measures and predicting the state of the system. Application of the results obtained in the process of building, operating and upgrading the information security for cloud services leads to increased efficiency and quality of service and allows to effectively manage the information security.

Keywords: *information security, dynamic perimeter, cloud environment, attacks on data*

DOI: 10.17587/it.24.791-798

References

1. **Analysis** of Cloud related Security and risks mitigation IRACST, *International Journal of Advances Computing, Engineering and Applications (IJACEA),* 2012, vol. 1, no. 2, pp. 40—49.

2. **Giunter E. S., Narutta N. N., Shahov V. G.** "Oblachnye" vychisleniia i problemy ikh bezopasnosti (Cloud Computing and Security Problems), *Omskii Nauchnyi Vestneyk*, 2013, no. 2 (120), pp. 279—282.

3. **Saclakov V. M.** Oblachnye vychisleniia: sovremennye modeli predostavleniia uslug i vozmozhnye riski (Cloud computing: modern service delivery models and possible risks), *Molodezh i sovremennye informatcionnye tekhnologii: sbornik trudov XIII Mezhdunarodnoi nauchno-prakticheskoi konferentcii studentov, aspirantov i molodykh uchenykh, g. Tomsk, 9—13 noiabria 2015 g.* Tomsk, Publishing house of TPU, 2016, vol. 2, pp. 104—106 (in Russian).

4. **Frolov D. B., Gruniushkina S. A., Starostin A. V.** *Informatcionnaia geo-politika i set Internet* (Information geopolitics and the Internet), Moscow, RFK-Imidzh Lab, 2008, 404 p. (in Russian).

5. **Iusupov R. M., Shishkin V. M.** O nekotorykh protivorechiiakh v reshenii problem informatcionnoi bezopasnosti (On some contradictions in solving information security problems), *Trudy SPIIRAN*, 2008, no. 6, pp. 11—23 (in Russian).

6. **Petrov D. L.** Optimalnyi algoritm migratcii dannykh v masshtabiruemykh oblachnykh khranilishchakh (The optimal algorithm for data migration in scalable cloud storage), *Upravlenie bolshimi sistemami: sbornik trudov*, 2010, no. 30 (in Russian).

7. **Vorobev V. I., Ryzhkov S. R., Fatkieva R. R.** Zashchita perimetra oblachnykh vychislenii (Protecting the perimeter of cloud computing), *Programmnye sistemy: teoriia i prilozheniia*, 2015, vol. 6, no. 1 (24), pp. 61—71 (in Russian).

8. **Kovalenko O. S.** Obzor sostoianii, problem i perspektiv khraneniia i analiza dannykh v "oblake" (Overview of the states, problems and perspectives of data storage and analysis in the "cloud"), *Informatika, Vychislitelnaia Tekhnika i Inzhenernoe Obrazovanie*, 2011, no. 5, pp. 39—49 (in Russian).

9. **Kamenshchikov A. A.** Oblachnye tekhnologii i interoperabelnost informa-tcionnykh sistem v zdravookhranenii (Cloud technologies and interoperability of information systems in healthcare), *Zhurnal Radioelektroniki*, 2013, no. 2, available at: http://j re.cplire.ru/j re/feb 13/11/text.pdf. Version 2018/06/28 15: 01 (in Russian).

10. **Chemerkin Iu. S.** Oblachnye vychisleniia kak instrument obrabotki konfidentcialnoi informatcii (Cloud computing as a tool for processing confidential information), *Vestneyk RGGU. Seriia: Dokumentovedenie i arhivovedenie. Informatika. Zashchita informatcii i informatcionnaia bezopasnost*, 2012, no. 14, pp. 53—65 (in Russian).

11. **Mauw S., Verschuren J. H. S., de Vink E. P.** A formalization of anonymity and onion routing, *Computer Security—ESORICS 2004*, Springer Berlin Heidelberg, 2004, pp. 109—124.

12. **Gupta S., Kumar P.** Taxonomy of cloud security, *International Journal of Computer Science, Engineering and Applications (IJCSEA),* October 2013, vol. 3, no. 5, pp. 47—67.

13. **Lonea A. M., Popescu D. E., Tianfield H.** Detecting DDoS attacks in cloud computing environment, *International Journal of Computers Communications & Control*, 2013, vol. 8, pp 70—78.

14. **Simma A.** Trusting Your Cloud Provider: Protecting Private Virtual Machines, *Magdeburger Journal zur Sicherheitsforschung,* Vol. 1, pp. 530—539. Retrieved June 17, 2015, URL: http://www. sicherheitsforschung-magdeburg. de/publikationen. html Version 2015/06/16 20: 01. — 2015.

15. Pivoting in Amazon Clouds available at: http://andresriancho.github.io/nimbostratus/pivoting-in-amazon-clouds.pdf html Version 2013/10/27 20: 48. — 2013.

16. **Adrian D.** et al. Imperfect forward secrecy: How Diffie-Hellman fails in practice, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM*, 2015, pp. 5—17.

17. **Osipov V. Iu., Nosal I. A.** Obosnovanie meropriiatii obespecheniia informatcionnoi bezopasnosti (Rationale for measures to ensure information security), *Informatcionno-Upravliaiushchie Sistemy*, 2013, no. 2 (63), pp. 48—53 (in Russian).

18. **Osipov V. Iu., Nosal I. A.** Obosnovanie perioda peresmotra meropriiatii po zashchite informatcii (Justification of the revision period for information protection measures), *Informatcionno-Upravliaiushchie Sistemy*, 2014, no. 1, pp. 63—69 (in Russian).

19. **Potapov V. I.** Postanovka i reshenie igrovoi zadachi protivoborstva apparatno-izbytochnoi dinamicheskoi sistemy s atakuiushchim protivnikom, deistvuiushchim v usloviiakh nepolnoi informatcii v protcesse konflikta (Statement and solution of the game problem of confrontation of the hardware-redundant dynamic system with the attacking enemy operating under incomplete information in the process of conflict), *Mekhatronika, Avtomatizatsiya, Upravlenie*, 2017, vol. 18, no. 8, pp. 525—531 (in Russian).