REFERENCES:

1. *Modestov A. A., Belyaeva E. A.* Integrated assessment of features for hardware-software unites of trusted boot // Vestnik RosNOU. 2013. № 4. P. 105–107.
2. *Modestov A. A., Belyaeva E. A.* Integrirovannaya otsenka funktsionalnyh vozmozhnostey apparatno-programmnyh moduley avtorizovannoy zagruzki // Spetstehnika i svyaz. 2013. № 6. P. 61–63.

*L. R. Tuliganova, I. V. Mashkina*

**Numerical Assessment Risk Breaches of Information Security in the Virtualization Sector of an Enterprise Information System**

*Key words: virtualization technology, threat model, numerical value of the risk*

This research is devoted to the calculation of numerical values of the risk of information security breaches in the virtualization sector of an enterprise information system. To obtain numerical values of risk it is necessary to build a detailed model of threats. The result shows that when using virtual means of protection there is a possibility to reduce the value of risk.

*Л. Р. Тулиганова, И. В. Машкина*

## ЧИСЛЕННАЯ ОЦЕНКА РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕГМЕНТЕ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ[2]

В настоящее время технология виртуализации становится все более популярной. Используя технологию виртуализации, предприятия могут сократить расходы на развитие и поддержку своей физической инфраструктуры, обеспечить непрерывность бизнес-процессов, упростить администрирование.

При использовании технологии виртуализации в информационных системах (ИС) предприятий руководство сталкивается с проблемой обеспечения информационной безопасности (ИБ). Для обеспечения безопасности данных в кластере виртуализации должны быть определены, в первую очередь, требования к системе защиты. Меры по защите среды виртуализации должны исключать несанкционированный доступ к компонентам виртуальной инфраструктуры и к информации, обрабатываемой в виртуальной среде.

Для определения адекватности и полноты используемых мер защиты осуществляется оценка риска нарушения ИБ в сегменте виртуализации. Для получения численной оценки риска необходимо выявить потенциально возможные угрозы в среде виртуализации и уязвимости на путях их распространения. В работе предложена детализированная модель угроз в среде виртуализации. При построении модели угроз используется информация об инфраструктуре сегмента виртуализации и ИС в целом, об источниках и объектах возможных атак, о правах доступа и установленных средствах защиты. Модель разработана с учетом угроз несанкционированного доступа к сети передачи данных и информации, обрабатываемой в виртуальной среде, к компонентам виртуальной инфраструктуры, в том числе к средствам управления виртуальной

[2] Работа выполнена при поддержке гранта РФФИ № НЧ-НЧ-05-14-ГФ.

инфраструктурой, гипервизору, образам виртуальных машин и системе хранения данных, хостовым и гостевым операционным системам.

Используется метод расчета рисков, предложенный в [1], адаптированный для применения в среде виртуализации. В качестве объектов атак $O_i (i \in 1,3)$ приняты: базы данных и образы виртуальных машин на Storage System Server, системное программное обеспечение — гипервизор I типа, работающий экземпляр виртуальной машины на сервере вычислительного кластера. В качестве источников угроз $S_j (j \in 1,3)$ рассмотрены: пользователь физической сети, неавторизованный для работы в виртуальном сегменте, сотрудник-пользователь виртуального сегмента, работающий на одном физическом сервере с атакуемой виртуальной машиной и сотрудник- пользователь виртуального сегмента, атакующий виртуальную машину, запущенную на другом физическом сервере. Веса промежуточных концептов $w_{z,z+1}$ между источниками угроз и объектами атак — это уязвимости аппаратуры связи, физических и виртуальных средств защиты, механизмов защиты операционной системы. Каждому промежуточному концепту соответствует значение уязвимости из Международной базы данных National Vulnerability Database [2].

От одного источника угрозы к одному объекту атаки может быть как один, так и несколько путей реализации угроз. К одному объекту атаки возможны угрозы как от одного, так и от нескольких источников атак. Вероятность угрозы на одном пути реализации, от одного источника к одному объекту $\rho_{ij}$, вычисляется как произведение весов уязвимостей промежуточных концептов и вероятности активизации данного пути. Результирующая вероятность угрозы к $i$-му информационному объекту определяется с учетом общего количества источников атак. Для дальнейших расчетов выбирается тот путь от источника к объекту, которому соответствует наибольшее значение вероятности.

Расчетный пример показал возможность повышения защищенности сегмента виртуализации ИС в 1,7 раза за счет использования виртуальных средств защиты Virtual Firewall/VPN и Virtual IPS, значения уязвимостей которых в [2] соответствуют 0,49 и 0,68.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Гузаиров М. Б., Машкина И. В., Степанова Е. С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. № 2. С. 37–49.
2. National Vulnerability Database. URL: http://nvd.nist.gov/ (дата обращения: 25.11.2014).

## REFERENCES:

1. *Guzairov M. B., Mashkina I. V., Stepanova E. S.* Postroenie modeli ugroz s pomoshch'yu nechetkikh kognitivnykh kart na osnove setevoi politiki bezopasnosti // Bezopasnost' informatsionnyh tekhnologii. 2011. № 2. P. 37–49.
2. National Vulnerability Database. URL: http://nvd.nist.gov/ (data obrashcheniya: 25.11.2014).