5. *Zaytsev A. S., Malyuk A. A.* Issledovanie problemy vnutrennego narushitelya // Vestnik RGGU. 2012. № 14. P. 117–133.
6. *Gurin S. I.* Osnovy protivodeystviya insayderskim ugrozam. M.: NRNU MEPHI, 2013.
7. *Atamanov A. N.* Voprosy otsenki riskov informatsionnoy bezopasnosti v avtomatizirovannyh sistemah // Sovremennaya nauka: Aktualnye problem teorii i praktiki. 2012 URL: http://www.nauteh-journal.ru/index.php/ru/----etn12-02/371-a
8. *Bidyuk P. I., Terentyev A. N.* Postroenie i metody obucheniya Bayesovskih setey // Tavricheskiy vestnik informatiki i matematiki. 2004. № 2. P. 1–3.
9. *Neal R. M., Hilton G. E.* A view of the EM algorithm that justifies incremental, sparse, and other variants. University of Toronto, 1999.
10. *Greitzer F. L., Paulson P. R., Kangas L. J., Franklin L. R., Edgar T. W., Frincke D. A.* Predictive Modeling for Insider Threat Mitigation. Richland. WA: Pacific Northwest National Laboratory, 2009.

A. A. Modestov, E. A. Belyaeva

Valuation Method for Hardware-Software Unites of Trusted Boot

Key words: feature, integrated assessment, expertise, unauthorized access

The science-based approach to obtaining integrated assessment of features for hardware-software unites of trusted boot based on an algorithm of receiving a comprehensive measure to assess the effectiveness of protection against unauthorized access and comparative evaluation methodology by "cost — effectiveness is presented by the authors of the article.

А. А. Модестов, Е. А. Беляева

МЕТОДИКА ОЦЕНКИ АППАРАТНО-ПРОГРАММНЫХ МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ[1]

Рассматривается наиболее широко применяемый класс аппаратно-программных средств защиты информации — аппаратно-программные модули доверенной загрузки (АПМДЗ). Проблема обеспечения научно обоснованного выбора АПМДЗ для решения задач по защите от НСД решается путем разработки научно обоснованной методики получения комплексной оценки функциональных возможностей АПМДЗ, позволяющей выявить АПМДЗ с наилучшими характеристиками обеспечения защиты информации от НСД.

Пусть $A = \{A_i\}$ — множество АПМДЗ, $S = \{S_i\}$ — множество стоимостей АПМДЗ. Каждый АПМДЗ $A_i \in A$ характеризуется: $V_{main} = \{V^j_{main}\}$ — множеством основных функциональных возможностей, $V_{add} = \{V^l_{add}\}$ — множеством дополнительных функциональных возможностей. $E(A_i) = f(V_{main}, V_{add})$, S — критерий эффективности АПМДЗ A_i в части обеспечения защиты обрабатываемой информации от НСД.

Найти такие $A' \in A$, при которых: $E(A') = f(V_{main}(A'), V_{add}(A'), S(A')) = \max(E(A_i))$ [1].

Разработанный алгоритм получения значения показателя для оценки функциональных возможностей АПМДЗ, в зависимости от типа оцениваемых функциональных возможностей (основные или дополнительные), включает в себя следующие этапы:

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполненного совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050

Этап 1. Выбор АПМДЗ для оценивания.

Этап 2. Выбор типа функциональных возможностей для оценивания.

Этап 3. Оценивание АПМДЗ в соответствии с выбранными типами функциональных возможностей.

Согласно алгоритму получения значений показателей для оценки функциональных возможностей АПМДЗ показатель комплексной оценки АПМДЗ $E(A)$ по критерию «эффективность-стоимость» вычисляется по следующей формуле:

$$E(A)=\frac{\sum_{m=1}^{|M|}R_m\left(\sum_{i=1}^{|K_{main}|}\left|V_{K^i_{main}}\right|\sum_{l=1}^{}\varphi(V^l_{K^l_{main}})E(V^l_{K^l_{main}})\psi(K^i_{main})+\sum_{j=1}^{|K_{add}|}\left|V_{K^j_{add}}\right|\sum_{n=1}^{}\varphi(V^n_{K^n_{add}})E(V^n_{K^n_{add}})\psi(K^j_{add})\right)}{S(A)\sum_{m=1}^{|M|}R_m},$$

где

K_{main} — набор классификационных признаков оценки основных функциональных возможностей АПМДЗ A;

R_m — ранг предпочтительности оценок, полученных m-м экспертом;

M — множество экспертов, входящих в экспертную группу;

K_{add} — набор классификационных признаков оценки дополнительных функциональных возможностей АПМДЗ A;

$E(K)$ — показатель оценки эффективности реализации функциональных возможностей по классификационному признаку K АПМДЗ A;

$E(V)$ — показатель оценки эффективности реализации функциональной возможности V АПМДЗ A;

$\varphi(V)$ — ранг предпочтительности функциональной возможности V;

$\psi(K)$ — ранг предпочтительности классификационного признака K.

Предлагаемая методика сравнительной оценки функциональных возможностей АПМДЗ состоит из следующих этапов:

Этап 1. Выбор множества $A=\{A_i\}$ АПМДЗ для сравнения.

Этап 2. Выбор группы экспертов для оценивания заявленного множества АПМДЗ.

Этап 3. Ранжирование группы экспертов.

Этап 4. Выдача анкет.

Этап 5. Заполнение анкет экспертами.

Этап 6. Сбор анкет экспертов для дальнейшей обработки.

Этап 7. Подсчет показателя комплексной оценки функциональных возможностей АПМДЗ.

Этап 8. Из всех $A_i \in A$ выбирается

$$A': E(A')=\max_{A_i\in A}(E(A_i))$$ [2].

Методика сравнительной оценки функциональных возможностей АПМДЗ, основанная на классификации функциональных возможностей, позволяет из совокупности АПМДЗ выявить модуль с наилучшими характеристиками обеспечения защиты информации от НСД.

СПИСОК ЛИТЕРАТУРЫ:

1. *Модестов А. А., Беляева Е. А.* Комплексная оценка функциональных возможностей аппаратно-программных модулей доверенной загрузки // Вестник РосНОУ. 2013. № 4. С. 105–107.

2. *Модестов А. А., Беляева Е. А.* Интегрированная оценка функциональных возможностей аппаратно-программных модулей авторизованной загрузки // Спецтехника и связь. 2013. № 6. С. 61–63.

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.