

И. В. КОТЕНКО, М. В. СТЕПАШКИН, Д. И. КОТЕНКО, Е. В. ДОЙНИКОВА

## ОЦЕНИВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ПОСТРОЕНИЯ ДЕРЕВЬЕВ СОЦИОИНЖЕНЕРНЫХ АТАК

Представлен подход к оценке защищенности информационных систем на основе построения деревьев атак, являющийся развитием подхода, предложенного авторами ранее (введены понятия, модели и конструкции, связанные с возможностью учета социоинженерных атак).

*Ключевые слова:* защита информации, анализ защищенности, информационная система, социоинженерные атаки, показатель защищенности.

**Введение.** Одной из актуальных задач защиты информации является анализ защищенности информационных систем (ИС). В большинстве предлагаемых для решения этой задачи методик рассматриваются только программно-технические (ПТ) атаки, использующие известные уязвимости в программном и аппаратном обеспечении, однако не учитывается, что успешная реализация социоинженерных (СИ) атак обеспечивает злоумышленнику плацдарм для проведения программно-технических атак и приносит зачастую значительно больший ущерб.

Представленный в настоящей работе подход к анализу защищенности ИС, предназначенный для использования в перспективных системах анализа защищенности (САЗ), является развитием предложенного авторами ранее [1, 2] подхода к анализу защищенности, в нем введены понятия, модели и конструкции, позволяющие учитывать СИ-атаки.

**Релевантные работы.** Анализу защищенности систем посвящено большое количество работ, одной из его важнейших задач является классификация нарушителей и построение модели нарушителя [3].

Использованию графов и деревьев атак при анализе защищенности также посвящено множество работ: в [4] для анализа уязвимостей используется проверка на модели; в [5] предлагается подход к созданию графов атак; в [6] разрабатываются методика и инструментарий для анализа уязвимостей; в [7] описан подход к оценке уровня риска критических сетевых ресурсов на основе поведенческих графов атак и байесовского метода; в [8] предлагаются общая схема и алгоритмы ранжирования графов атак.

В работе [9] определены две основные категории методов реализации социоинженерных атак, нацеленных на „машину“ или „человека“ (computer-based и human-based); в [10] предложена классификация атак, основанных на методах социотехники.

Предлагаемый в настоящей работе подход к оценке защищенности базируется на концепциях, моделях и методиках, представленных в указанных выше работах. Основным его отличием является возможность получения результатов анализа защищенности (множества показателей защищенности) путем построения и анализа дерева атак, в котором наряду с

программно-техническими атаками, направленными на технические средства ИС, представлены социоинженерные атаки, объектами которых являются санкционированные пользователи.

**Функциональная архитектура перспективной САЗ** представлена на рис. 1. Приведем основные функциональные узлы данной архитектуры.

1) *Администратор ИС* — должностное лицо, ответственное за формирование модели (спецификации) ИС, обновление баз данных ПТ-атак, планирование внедрения новых средств защиты информации (СЗИ).

2) *Администратор безопасности ИС* — должностное лицо, ответственное за разработку модели нарушителя, политики безопасности информации, расширение модели ИС в части вопросов защиты информации от несанкционированного доступа, а также формирование требований к показателям защищенности (ПЗ) ИС.

3) *Проектировщик ИС* — должностное лицо, выполняющее функции технического администратора и администратора безопасности проектируемой ИС.

4) *Система анализа защищенности* позволяет строить и анализировать дерево атак на основе имитации атакующих действий нарушителя, направленных как на технические средства ИС, так и на ее санкционированных пользователей.

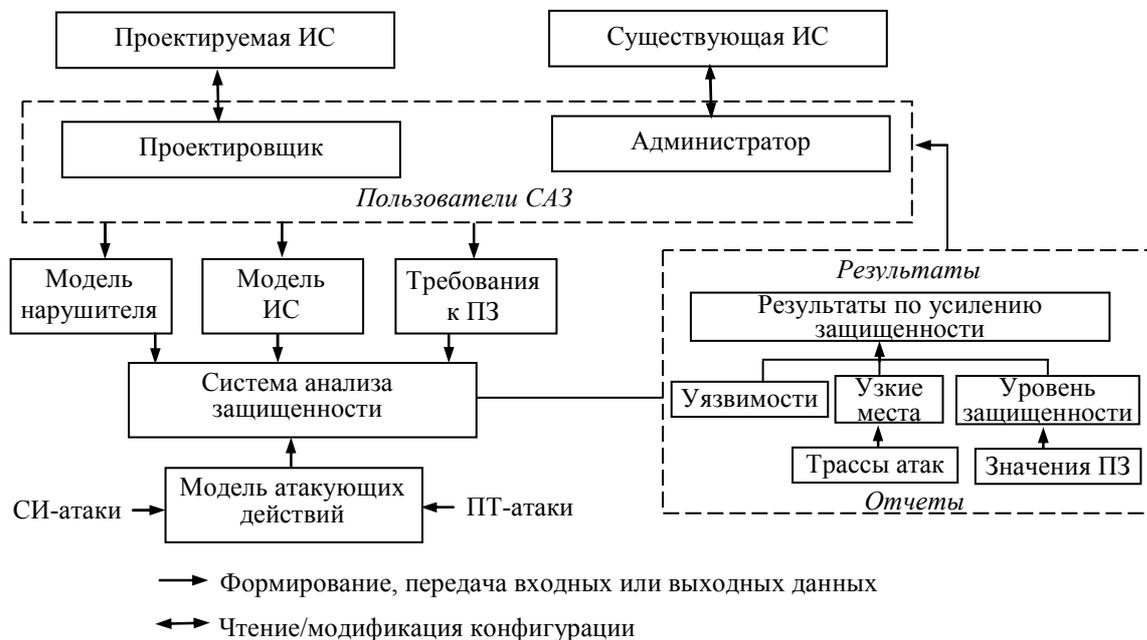


Рис. 1

*Процесс анализа защищенности* состоит из следующих этапов:

1) подготовительный (выполняется администраторами или проектировщиком ИС) — включает определение и документирование ресурсов ИС, их атрибутов (например, уровень критичности), используемых СЗИ, предъявляемых требований к уровню защищенности ИС, реализуемой политики безопасности, включающей описание модели нарушителя и т.д.;

2) инициализация (выполняется САЗ на основе полученных от пользователей данных) — включает формирование внутренних представлений моделей ИС и нарушителя, обновление внутренней базы данных уязвимостей;

3) построение дерева атак и его анализ (реализуется САЗ по команде пользователя);

4) анализ полученных результатов и выполнение пользователями САЗ рекомендаций по усилению защищенности.

**Модели анализа защищенности ИС.** Для формирования модели ИС предлагается расширить существующие модели компьютерных сетей [12, 13] путем добавления следующих классов объектов:

1) *контролируемая зона* — пространство, в котором регламентировано пребывание сотрудников и посетителей организации, а также различных технических средств;

2) *санкционированный пользователь* — должностное лицо, имеющее доступ в определенные контролируемые зоны, к заданным вычислительным платформам и информационным объектам, идентифицируемое при выполнении доступа по уникальному идентификатору. При успешной атаке нарушитель может получить доступную санкционированному пользователю информацию об ИС;

3) *группа санкционированных пользователей* — класс, используемый с целью упрощения таблиц дискреционного управления доступом;

4) *информационный объект* — абстракция, позволяющая представить некоторую совокупность обрабатываемой в ИС информации, доступ к которой контролируется правилами дискреционной политики управления доступом (файл в файловой системе вычислительной платформы и т.п.).

В качестве базы для расширения моделей атакующих действий и нарушителя была взята модель, представленная в работе [2].

**Модель атакующих действий** предлагается расширить за счет добавления следующих классов атак: а) социоинженерные атаки и б) атаки, учитывающие физический доступ нарушителя к техническим средствам.

Множество потенциальных СИ-атак формируется экспертами, множество ПТ-атак строится на основе баз данных. Для описания атак используются предусловия и постусловия. Предусловия определяются с использованием основных понятий и положений теорий человеческих потребностей. На основе пирамиды (иерархии) потребностей А. Маслоу [11] может быть определен способ воздействия на санкционированного пользователя. В качестве постусловий выступают: получение нарушителем сведений, доступных санкционированному пользователю; согласие пользователя выполнять указания нарушителя.

Основное отличие ПТ- от СИ-атак заключается в том, что при успешной реализации ПТ-атаки нарушитель получает сведения только об атакуемой вычислительной платформе, а при успешной реализации СИ-атаки нарушитель может получить все сведения об ИС, известные пользователю.

Модель нарушителя состоит из следующих компонентов: первичные знания нарушителя об ИС (используемые ОС и приложения, топология и т.д.); технические знания и умения нарушителя, определяющие его возможности по реализации ПТ-атак (в первую очередь, по компилированию и использованию программного кода, реализующего атаки); первоначальное положение относительно системы (внутренние и внешние нарушители).

Расширение модели нарушителя обеспечивает возможности задания:

— объектов новых классов (контролируемые зоны, информационные объекты и т.д.) в качестве первичных знаний нарушителя;

— множества „замаскированных“ под санкционированных пользователей ИС нарушителей;

— ресурсов (в том числе финансовых), которые обеспечивают нарушителю возможность реализации СИ-атак, направленных на санкционированных пользователей ИС.

**Модель определения уровня защищенности ИС** базируется на использовании оценки критичности атакующего действия. Критичность ПТ-атак рассчитывается на основе интегрального базового индекса CVSS [14] атакующего действия и методики анализа рисков FRAP [15]. Критичность СИ-атаки определяется экспертным путем.

Получение качественной экспресс-оценки защищенности ИС (расчет общего уровня защищенности) осуществляется следующим образом:

1) вычисление показателей защищенности (критичность системы, сложность доступа и др.) различных объектов дерева атак (отдельных атакующих действий, трасс атак и угроз);

- 2) получение качественных оценок уровня риска для всех угроз;
- 3) расчет общего уровня защищенности анализируемой ИС на основе полученных оценок уровней риска всех угроз.

Отличие данной модели определения уровня защищенности ИС от модели, предложенной авторами ранее, заключается в том, что при выполнении расчетов в качестве атакуемого объекта может выступать как вычислительная платформа, так и санкционированный пользователь ИС.

**Системная архитектура перспективной САЗ.** С учетом предложенных моделей анализа защищенности и функциональной архитектуры перспективной САЗ была разработана ее системная архитектура, включающая:

- 1) программное средство „Конструктор спецификаций анализируемых ИС“, позволяющее пользователям САЗ формировать спецификации ИС с применением графического интерфейса;
- 2) программное средство „Система анализа защищенности ИС“, состоящее из клиентской (выполняет анализ защищенности ИС, заданной в виде подготовленной заранее спецификации, рис. 2) и серверной (обеспечивает обработку сведений об уязвимостях программного и аппаратного обеспечения) частей;
- 3) программный компонент „Обновление базы данных уязвимостей“, обеспечивающий загрузку (актуализацию) сведений о ПТ-атаках из открытой базы данных уязвимостей National Vulnerability Database (NVD) [16].

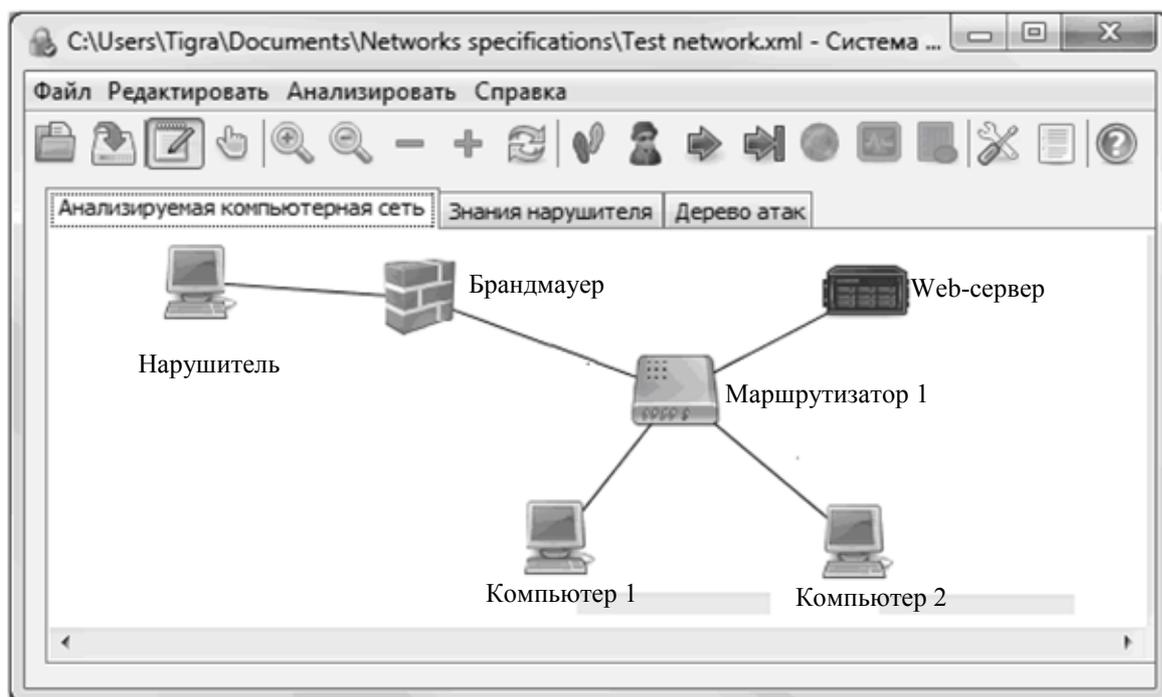


Рис. 2

**Заключение.** В работе представлен подход к анализу защищенности ИС с учетом СИ-атак, являющийся развитием предложенного авторами ранее подхода к анализу уязвимостей и оценке защищенности компьютерных сетей. Описаны расширения моделей информационной системы, атакующих действий, нарушителя и определения уровня защищенности (расчета множества показателей защищенности).

На основе предложенного подхода разработан прототип перспективной САЗ ИС, предназначенной для выполнения анализа защищенности на различных этапах жизненного цикла исследуемых информационных систем.

## СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Степашкин М. В., Богданов В. С. Анализ защищенности компьютерных сетей на различных этапах их жизненного цикла // Изв. вузов. Приборостроение. 2006. Т. 49, № 5. С. 3—8.
2. Котенко И. В., Степашкин М. В. Оценка защищенности компьютерных сетей на основе анализа графов атак // Проблемы управления рисками и безопасностью. Тр. Института системного анализа РАН. М., 2007. Т. 31. С. 126—207.
3. Phyo A. H., Furnell S. M. A Detection-oriented classification of insider IT misuse // Proc. of the Third Security Conf. Las Vegas, NV, 2004.
4. Ritchey R. W., Ammann P. Using model checking to analyze network vulnerabilities // Proc. of the 2000 IEEE Symp. on Security and Privacy. Washington, DC, 2000. P. 156—165.
5. Swiler L. P., Phillips C., Ellis D., Chakerian S. Computer-attack graph generation tool // DISCEX '01. Proc. Anaheim, CA, 2001. Vol. 2. P. 307—321.
6. Rieke R. Tool based formal modelling, analysis and visualisation of enterprise network vulnerabilities utilising attack graph exploration // EICAR 2004. Conf. CD-rom: Best Paper Proc. 2004. P. 31—46.
7. Dantu R., Loper K., Kolan P. Risk management using behavior based attack graphs // Proc. of the Intern. Conf. on Information Technology: Coding and Computing. Washington, DC, 2004. Vol. 2. P. 444—449.
8. Mehta V., Bartzis C. et al. Ranking attack graphs // Lecture Notes in Computer Sci. Berlin: Springer-Verlag, 2006. Vol. 4219. P. 127—144.
9. A Proactive Defence to social engineering. SANS Institute InfoSec Reading Room [Электронный ресурс]: <[http://www.sans.org/reading\\_room/whitepapers/engineering/proactive-defence-social-engineering\\_511](http://www.sans.org/reading_room/whitepapers/engineering/proactive-defence-social-engineering_511)>.
10. How to protect insiders from social engineering threats. Midsize business security guidance [Электронный ресурс]: <<http://download.microsoft.com/download/4/7/>>.
11. Maslow A. H. A Theory of human motivation // Psychological Rev. 1943. Vol. 50. P. 370—396.
12. Morin B., Me L., Debar H., Ducasse M. M2d2: A formal data model for ids alert correlation // LNCS. Berlin: Springer-Verlag, 2002. Vol. 1516. P. 115—137.
13. Vigna G. A topological characterization of tcp/ip security: Techn. Report TR-96.156. Politecnico di Milano, 1996.
14. CVSS. Common Vulnerability Scoring System [Электронный ресурс]: <<http://www.first.org/cvss>>.
15. FRAP. Facilitated Risk Analysis Process [Электронный ресурс]: <<http://www.peltierassociates.com>>.
16. NVD. National Vulnerability Database [Электронный ресурс]: <<http://nvd.nist.gov>>.

**Сведения об авторах**

- Игорь Витальевич Котенко** — д-р техн. наук, профессор; СПИИРАН, лаборатория проблем компьютерной безопасности, Санкт-Петербург; заведующий лабораторией; E-mail: ivkote@comsec.spb.ru
- Михаил Викторович Степашкин** — канд. техн. наук; СПИИРАН, лаборатория проблем компьютерной безопасности, Санкт-Петербург; научный сотрудник; E-mail: stepashkin@comsec.spb.ru
- Дмитрий Игоревич Котенко** — аспирант; СПИИРАН, лаборатория проблем компьютерной безопасности, Санкт-Петербург; E-mail: dmitrykotenko1986@gmail.com
- Елена Владимировна Дойникова** — аспирант; СПИИРАН, лаборатория проблем компьютерной безопасности, Санкт-Петербург; E-mail: doynikova@comsec.spb.ru

Рекомендована лабораторией  
проблем компьютерной  
безопасности

Поступила в редакцию  
12.05.11 г.