УДК 004.056 Вестник УрФО № 2(20) / 2016, с. 33–38

**Соколов А. Н., Лужнов В. С.**

# *СПЕЦИАЛИЗИРОВАННЫЕ ИНСТРУМЕНТЫ АВТОМАТИЗИРОВАННОГО АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ*

*В работе рассмотрена проблема анализа защищенности автоматизированных систем, освещены нормативная и методическая базы в области аудита, аттестации и оценки информационной безопасности таких систем. Выполнен обзор рынка программных средств, реализующих на практике методики анализа защищенности, рассмотрены основные актуальные проблемы средств анализа защищенности и возможные перспективы их развития. На основе проведенного анализа и разработанного математического аппарата сформулирован алгоритм проведения в полуавтоматическом режиме анализа защищенности корпоративных автоматизированных систем. Преимущество предложенного алгоритма заключается в возможности проводить анализ защищенности автоматизированных систем на базе операционных систем Windows и UNIX с применением принципиально новой методологии определения уязвимостей и способов их устранения.*

***Ключевые слова:*** *информационная безопасность, автоматизированные системы, безопасность автоматизированных систем, анализ защищенности автоматизированных систем, аудит безопасности, атаки на информационные ресурсы, уязвимости системного программного обеспечения*

**N. Sokolov, V. S. Luznov**

# *SPECIALIZED TOOLS FOR AUTOMATED ANALYSIS OF INFORMATION SYSTEMS SECURITY*

*The paper considers the problem of security analysis of automated systems, illuminated by the regulatory and methodological framework in the field of audit, appraisal and evaluation of information security of such systems. Made a review of the software market, realizing in practice the techniques of security analysis, analyzed the basic topical problems of security analysis tools and possible prospects for their development. Developed an algorithm of the semi-automatic analysis of security of corporate automated systems, based on analysis of current software and developed mathematic model. The advantage of the proposed algorithm is the ability to analyze the security of automated systems based on Windows and UNIX*

*operating systems using a new methodology for determining and resection vulnerabilities of automated systems.*

***Keywords:*** *information security, automated systems, security, specialized software, security automation systems, security analysis of automated systems, security audit, attacks on information resources, the vulnerabilities of the system software.*

Тенденции развития систем автоматизации в настоящее время движутся в направлении создания таких систем, которые способны выполнять заданные функции или процедуры без участия человека (автоматических систем). Однако присутствие в решаемых задачах эвристических или сложно программируемых процедур объясняет широкое распространение полуавтоматических систем, так называемых автоматизированных систем [1]. Широкое распространение таких систем, их интенсивная интеграция в деятельность большинства государственных и коммерческих организаций приводит к тому, что от полноценного, стабильного и надежного функционирования автоматизированных систем, как государственных, так и коммерческих, напрямую зависит качество и результат всех процессов, происходящих в указанных организациях.

Одной из приоритетных задач при разработке автоматизированных систем является обеспечение их комплексной безопасности. В связи с этим к автоматизированным системам должны предъявляться особые требования по качественной и адекватной оценке степени защищенности всех процессов, протекающих в системе, оценке эффективности применяемых мер защиты информации, выявлению потенциальных уязвимостей в инструментах и средствах, т. е. по проведению полноценного анализа защищенности всей автоматизированной системы в целом. Под защищенностью автоматизированной системы здесь понимается степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации [2].

С учетом сложности и комплексности как самих процессов, так и применяемых мер защиты, процесс анализа защищенности без применения специализированных средств аудита, аттестации и обследования безопасности является на практике сложно осуществимым. В предложенной работе рассмотрены основные средства и инструменты, специально разработанные и предназначенные для проведения комплексного анализа защищенности автоматизированных систем, проблемы и перспективы их развития и использования.

Проведение мероприятий по организации защиты информации в автоматизированных системах и анализу степени эффективности этой защиты должно происходить в соответствии с принятыми в отрасли нормативными и методическими документами, в силу ценности защищаемой информации и объема потенциального ущерба от реализации в отношении нее тех или иных угроз. На международном уровне такими документами являются:

• общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation / ISO 15408). Стандарт содержит два основных вида требований безопасности: функциональные, предъявляемые к функциям безопасности и реализующим их механизмам, и требования доверия, предъявляемые к технологии и процессу разработки и эксплуатации;

• информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности (Information technology – Security techniques – Code of practice for information security management / ISO/IEC 17799). Стандарт предоставляет лучшие практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности.

В Российской Федерации к таким нормативным и методическим документам относятся:

• ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»;

• Руководящий документ (РД) «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);

• РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (1997);

• «Положение о сертификации средств защиты информации по требованиям безопасности информации» (Постановление Правительства РФ № 608, 1995 г.);

• РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (1992 г.);

• РД «Концепция защиты средств вычислительной техники от НСД к информации» (1992 г.);

• РД «Защита от НСД к информации. Термины и определения» (1992 г.);

• РД «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (1997 г.);

• РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (1999 г.).

Практической реализацией требований перечисленных документов являются специализированные программы и программные комплексы, которые, опираясь на критерии и параметры нормативов, предназначены для формирования качественной оценки защищенности автоматизированных систем.

На сегодняшний день подавляющее большинство программного обеспечения в сфере анализа защищенности вычислительных систем разрабатывается и распространяется за рубежом. Наиболее популярными программными средствами [2, 3] являются:

• Windows Security Scoring Tool (поставляемое для операционных систем семейства Windows NT средство анализа локальных политик безопасности. Позволяет осуществлять проверку соответствия настроек ОС MS Windows минимальному набору требований безопасности, определяющих базовый уровень защищенности, который в общем случае является достаточным для коммерческих систем);

• Security Configuration and Analysis Snap-In (стандартное средство операционной системы Windows для осуществления анализа и настройки параметров безопасности);

• NetRecon (сетевой сканер. Является инструментом администратора безопасности, предназначенным для исследования структуры сетей и 123 сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах);

• NESSUS (сетевой сканер. Предназначен для автоматического поиска известных изъянов в защите информационных систем. Способен обнаружить наиболее часто встречающиеся виды уязвимостей: наличие уязвимых версий служб или доменов, ошибки в конфигурации (например, отсутствие необходимости авторизации на SMTP-сервере), наличие паролей по умолчанию, пустых или слабых паролей);

• Enterprise Security Manager (автоматизированная система управления безопасностью предприятия);

• SAFEsuite (программные средства компании ISS (Internet Security Systems Inc.), предназначенные для анализа защищенности сетевых сервисов и протоколов Internet Scanner; операционных систем System Security Scanner; баз данных Database Scanner; обнаружения атак на сегменты и узлы сети RealSecure; поддержки принятия решения SAFEsuite Decisions).

На отечественном рынке в ходе его обзорного анализа среди всех представленных программных средств можно выделить программный комплекс «Сканер-ВС» [4] от разработчика «НПО Эшелон». Данный программный комплекс представляет собой дистрибутив операционной системы семейства GNU/Linux с предустановленным набором программного обеспечения для анализа отдельных аспектов защищенности автоматизированных систем [5], прошедший сертификацию ФСТЭК России и Министерства Обороны [6]. К его основным функциям относятся: определение топологии и инвентаризация ресурсов сети, поиск уязвимостей, локальный и сетевой аудит стойкости паролей, поиск остаточной информации на жестком диске, перехват и анализ сетевого трафика, аудит ПО и аппаратной конфигурации, контроль целостности, аудит WI-FI сетей, модуль гарантированной очистки информации.

Исходя из перечисленных выше фактов, можно сформулировать следующие актуальные проблемы в области программных средств анализа защищенности автоматизированных систем на отечественном рынке:

• нормативно-методическая база требует определенной актуализации;

• отсутствуют утвержденные уполномоченными органами методики анализа защищенности автоматизированных систем;

• малый объем рынка комплексных программных средств анализа защищенности;

• разобщенность действующих в отрасли стандартов и подходов к оценке защищенности автоматизированных систем;

• не полностью реализуемый потенциал разработчиков по заполнению рынка актуальными программными продуктами.

На пути решения перечисленных проблемных вопросов поставлена задача разработки комплексной методики анализа защищенности автоматизированных систем и ее практическая реализация в виде программного комплекса, способного учесть наиболее полные и актуальные мировые и отечественные практики в области обеспечения информационной безопасности автоматизированных систем. Методика базируется на математическом аппарате, который может быть реализован в виде ряда программных алгоритмов.

Математическая модель программного комплекса по анализу атак на информационные ресурсы автоматизированной системы [7] может быть представлена в виде графа $G = <L,E>$, где $L$ – множество вершин графа, а $E \subset L^2$ – множество дуг графа. Для графа G определено отношение $T \in \{E \times W\}$, которое каждой дуге из множества $E$ ставит в соответствие один или более элементов отношения $W$.

Предлагаемая модель атак на информационные ресурсы в своей основе состоит из трех базовых множеств: $V$ – множества уязвимостей информационных ресурсов автоматизированной системы, $A$ – множества способов реализации атак на информационные ресурсы, $C$ – множества последствий реализации атак на информационные ресурсы. Основные положения рассмотренной модели приведены в [8].

Для описания связей, существующих между элементами множеств $A$, $V$ и $C$, необходимо определить $n$-арное алгебраическое отношение (тернарное при $n = 3$) $W$ на множестве

$$W = A \times V \times C$$

Тогда элемент $(a, v, c)$, принадлежащий отношению $W$, где $a \in A$, $v \in V$, $c \in C$, в рамках модели представляет собой логическую структуру вида «Атака на информационные ресурсы, которая реализуется способом $a$ через эксплуатацию уязвимости $v$, приводящая к последствию $c$».

Использование отношения $T$ позволяет интерпретировать каждую дугу графа $G$ как один из типов моделируемой атаки на информационные ресурсы автоматизированной системы. При этом в отношении $T$ одной дуге $e \in E$ может соответствовать одновременно несколько элементов множества $W$ только при условии, что эти элементы обозначают атаки, приводящие к одним и тем же последствиям, т. е.:

$$(\forall e \in E), (\forall w' \in W), (\forall w'' \in W)\ \exists\ (e,w') \in T,$$
$$\exists\,(e,w'') \in T \leftrightarrow c' = c'',$$

где $w' = (a', v', c')$, $w'' = (a'', v'', c'')$ - элементы, принадлежащие множеству $W$, $a'$ и $a''$ – способы реализации атак, $v'$ и $v''$ – уязвимости, $c'$ и $c''$ – последствия реализации атак.

В каждую вершину графа $G$ может входить одновременно несколько дуг только при условии, что в отношении $T$ каждой такой дуге соответствуют элементы множества $W$, описывающие атаки на информационные ресурсы автоматизированной системы, которые приводят к одинаковым последствиям. Таким образом, вершины графа $G$ могут объединять различные этапы атаки на информационные ресурсы, приводящие к идентичным последствиям.

Пример описанного графа $G$ приведен на рис. 1.

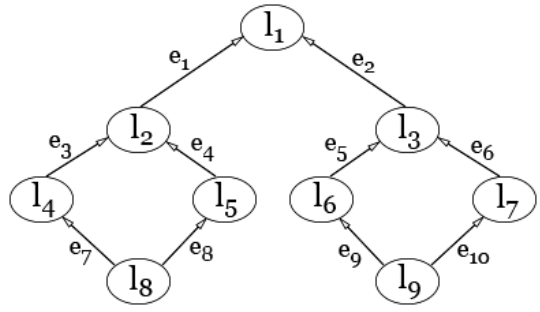


Рис. 1. Пример графа

На рис. 1: $l_1 \ldots l_9$ - вершины графа $G$, $e_1 \ldots e_{10}$ – дуги графа $G$. К графу применимо отношение $T$:

$$T = \{(e_1,(a_1,v_2,c_1)),(e_2,(a_2,v_1,c_1)),$$
$$(e_3,(a_2,v_1,c_2)),(e_4,(a_3,v_4,c_2)),$$
$$(e_5,(a_4,v_3,c_3)),(e_6,(a_5,v_5,c_3)),$$
$$(e_7,(a_5,v_6,c_4)),(e_8,(a_6,v_7,c_5)),$$
$$(e_9,(a_7,v_7,c_6)),(e_{10},(a_8,v_3,c_7))\}$$

Описанная математическая модель атак на информационные ресурсы автоматизированных систем может использоваться для реализации на ее основе алгоритмов и, как следствие, программного обеспечения, позволяющего проводить анализ защищенности автоматизированных систем.

Примером такого алгоритма анализа защищенности может выступать следующий набор инструкций:

1. Для построения модели атак на информационные ресурсы составляются списки уязвимостей, способов реализации угроз и последствий от их реализации. Данные списки выступают основой для формирования множеств $V, A, C$.

2. Исходя из условий $0 < |A_i| < |A|, 0 < |V_j| < |V|, 0 < |C_j| < |C|, 0 < |A_k| < |A|$ и $W = A \times V \times C$, формируется множество всех возможных комбинаций из элементов множеств $V, A, C$.

3. Полученное множество подвергается фильтрации для исключения из него элементов, не соответствующих тернарному отношению $W = A \times V \times C$.

4. По результату фильтрации формируется множество $W'$, содержащее в себе возможные и невозможные элементы-сочетания $(a_i, v_j, c_k)$. Для исключения из $W'$ элементов, описывающих невозможный сценарий атаки, проводится второй этап фильтрации. Для его реализации формируются множества элементов $(a,v)$, $(a,c)$, $(v,c)$, описывающие невозможные сочетания атак и уязвимостей, атак и последствий, уязвимостей и последствий соответственно.

5. На основе сформированных множеств множество $W'$ фильтруется до состояния $W$, пригодного для построения модели атак.

6. На основе множества $W$ строится граф $G = < L,E >$ путем формирования множества $T \in \{E \times W\}$ с учетом правила, что в отношении $T$ одной дуге $e \in E$ могут соответствовать одновременно несколько элементов множества $W$ только при условии, что эти элементы обозначают атаки, приводящие к одним и тем же последствиям.

7. В результате множество $T$ содержит в себе все возможные сценарии проведения атак на информационные ресурсы. Для реализации анализа защищенности каждому из последствий множества C задается вес r, прямо пропорциональный ущербу ресурсам системы от наступления последствия, такой, что $0 < r_i < 1$ и $\sum_1^i r_i = 1$, т. е. каждое последствие имеет вес, отличный от нуля, при этом суммарный вес всех последствий не превышает 1.

Приведенный алгоритм может быть формализован в виде схемы по ГОСТ 19.701-90 в виде схемы алгоритма (рис. 2).

Описанный алгоритм на момент проведения данного анализа находится на стадии реализации в виде прикладного программного обеспечения для операционных систем семейства Windows и UNIX, разрабатываемый на языке C++ для обеспечения эффективной скорости работы и необходимого уровня кроссплатформенного переноса программного кода. С учетом проведенного анализа рынка описанный в работе алгоритм представляется перспективным направлением разработок, способным обеспечить компенсацию основных узких моментов функционирования существующих программных средств.

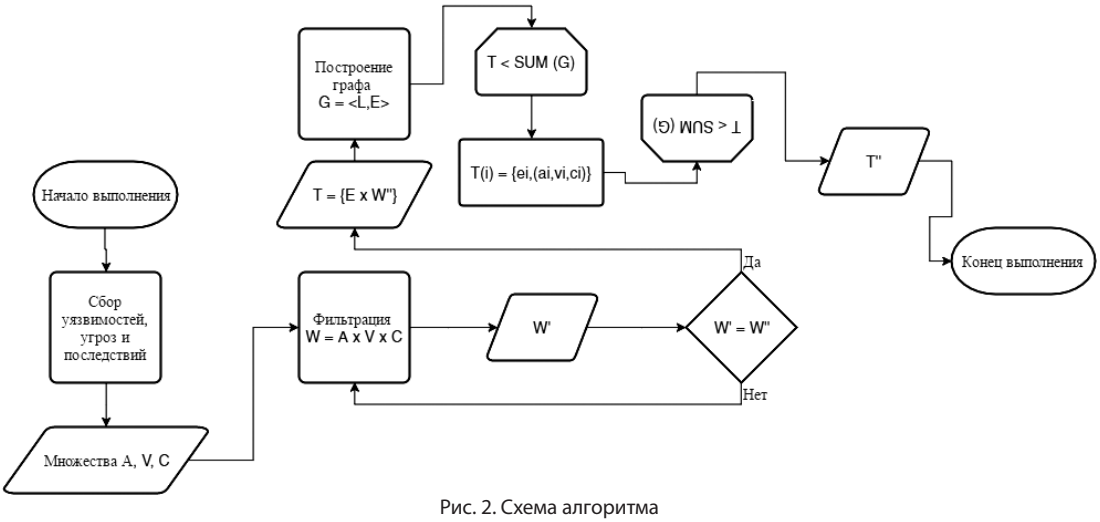


Рис. 2. Схема алгоритма

**Примечания**

1. Капустин, Н. М. Автоматизация производственных процессов в машиностроении: Учеб. для втузов / Под ред. Н. М. Капустина. – М.: Высшая школа, 2004. – 415 с.

2. Астахов А. Анализ защищенности корпоративных автоматизированных систем. / А. Астахов. // Информационный бюллетень Jet Info №7 (110)/2002. – Режим доступа: http://www.jetinfo.ru/Sites/new/Uploads/2002_7.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf, свободный. – Загл. с экрана.

3. Суханов А.В. Автоматизированные средства анализа защищенности информационных систем. / А.В. Суханов. // Журнал научных публикаций аспирантов и докторантов, 2008 – Режим доступа: http://www.jurnal.org/ articles/2008/inf31.html, свободный. – Загл. с экрана.

4. Средство анализа защищенности «Сканер-ВС». / Электрон. дан. – М.: ЗАО «НПО Эшелон», 2012. – Режим доступа: http://scaner–vs.ru/, свободный. – Загл. с экрана.

5. Программный комплекс «Средство анализа защищенности «Сканер- ВС». Описание программы. / Электрон. дан. – М.: ЗАО «НПО Эшелон», 2012. – Режим доступа: http://scaner-vs.ru/data/description_sca.pdf, свободный. – Загл. с экрана.

6. Разработки НПО «Эшелон». Сканер-ВС. / Электрон. дан. – М.: ЗАО «НПО Эшелон», 2014. – Режим доступа: http://www.npo-echelon.ru/ production/65/4291, свободный. – Загл. с экрана.

7. Лужнов В.С., Соколов А.Н. Анализ защищенности корпоративных автоматизированных систем на основе модели атак на информационные ресурсы / В.С. Лужнов, А.Н. Соколов. I Международная научно–техническая конференция «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах «Информ–2015»: сборник трудов. – Курск: Изд–во КГУ, 2015

**Соколов Александр Николаевич,** кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), г. Челябинск. E-mail: ANSokolov@inbox.ru

**Лужнов Василий Сергеевич,** аспирант, ассистент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: ua9stz@gmail.com.

**Alexander Sokolov,** a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru

**Vasiliy Luzhnov,** Graduate Student, Assistant of the Department «Information Systems Security», South Ural State University, Chelyabinsk, Russian Federation. E-mail: ua9stz@gmail.com