УДК 004.414

О. О. Карпова, соискатель, Пермский государственный технический университет
Л. Н. Кротов, доктор физико-математических наук, профессор, Пермский государственный технический университет
Е. Л. Кротова, кандидат физико-математических наук, Пермский государственный технический университет
А. Э. Осипович, студент, Пермский государственный технический университет

ПОДХОД К ПОСТРОЕНИЮ МОДЕЛИ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА*

Представлены основные задачи, которые необходимо решить при построении модели защиты автоматизированной системы от несанкционированного доступа. Формулируется часть задания для разработки программного обеспечения, необходимого для решения одной из поставленных задач.

Ключевые слова: математическое моделирование, теория автоматического управления, защита информации.

В настоящее время в современном обществе во главу угла ставится эффективность производства, которой невозможно добиться без актуальной, целостной информации. Автоматизация процессов позволяет достичь результата в кратчайшие сроки и с гораздо меньшими затратами ресурсов либо может показать, что какое-либо действие будет неэффективным, то есть появится аргументация в пользу необходимости поиска новых, альтернативных методов решения проблемы. Управление процессом также играет немаловажную роль в жизни предприятия, ведь на этот вид деятельности также тратятся время и ресурсы.

Наличие двух составляющих для автоматизации, а именно производственного процесса и управления этим процессом, дает возможность рассматривать целесообразность создания автоматизированной системы для решения задачи оптимизации затрат времени и ресурсов предприятия. С одной стороны, переход на уровень автоматизированной системы решает ряд существенных задач, с другой – порождает новые проблемы в виде угроз безопасности обрабатываемой информации.

Сегодня выделяются следующие основные виды угроз безопасности автоматизированной системы:

- угроза, проявляющаяся при аутентификации пользователя автоматизированной системы [1];
- угроза конфиденциальности информации;
- угроза доступности информации;
- угроза утраты целостности информации.

Все перечисленные угрозы имеют своей основой несанкционированный доступ к автоматизированной системе. Исходя из угроз безопасности можно выделить четыре основных задачи обеспечения безопасности автоматизированной системы:

1) обеспечение успешной аутентификации легального пользователя автоматизированной системы;
2) конфиденциальности информации;
3) доступности информации;
4) целостности информации.

Для решения задач обеспечения безопасности целесообразно построить модель защиты автоматизированной системы. Решение всех четырех задач сразу является нетривиальной многопараметрической задачей, следовательно, имеет смысл выделить наиболее важные для конкретного типа автоматизированной системы задачи, на решении которых можно будет построить модель защиты.

Первоначально в качестве приоритетной задачи для построения модели защиты, предполагается выделить задачу обеспечения успешной аутентификации легального пользователя автоматизированной системы.

Для решения этой задачи, а также в целях сведения к минимуму возможности проникновения в систему злоумышленника необходимо использовать криптостойкие протоколы [2].

Для создателей модели является неважным, что именно будет использоваться в качестве информации, идентифицирующей пользователя, будь то ставшая уже стандартной схема с именем пользователя (логином) и паролем, электронные идентификаторы или биометрическая информация, ведь любой алгоритм аутентификации сводится к проверке полученных данных для установления подлинности субъекта.

Сегодня алгоритмы, которые бы использовали передачу данных без шифрования, уже не используются. Однако даже алгоритмы, использующие ставшие уже традиционными схемы шифрования данных, в настоящее время стремительно теряют стойкость (например, стойкость системы RSA падает примерно в 30 раз за год). Стандартный метод повышения стойкости алгоритма – увеличение длины ключа, с помощью которого шифруются данные, но у этого метода есть существенный недостаток – происходит также усложнение шифрования. Путем решения проблемы обеспечения той же криптостойкости системы при меньшей длине ключа можно обозначить использование алгоритмов, которые используют теорию эллиптических кривых.

В 80-е годы прошлого века теория эллиптических кривых получила приложения в области построения алгоритмов факторизации больших чисел, и через эти приложения вошла в криптографию.

Получено 27.06.11
* Работа выполнена при финансовой поддержке гранта РФФИ – Урал № 11-01-96015.

В криптографии с открытым ключом эллиптические кривые являются основой ряда алгоритмов ECC – криптографии на эллиптических кривых. Ряд авторов для краткости называют ее просто эллиптической криптографией [3]. Интерес в криптографии к эллиптическим кривым обусловлен, с одной стороны, тем, что они являются богатым источником конечных абелевых групп, обладающих полезными структурными свойствами, с другой – тем, что на их основе обеспечиваются те же криптографические свойства, которыми обладают числовые или полиномиальные криптосистемы, но при существенно меньшем размере ключа.

Для решения задачи создания модели защиты автоматизированной системы от несанкционированного доступа предполагается построить математическую модель защиты автоматизированного рабочего места, которая будет включать в себя комплекс программ либо программную среду. Перед началом выполнения работы необходимо выделить существенные для построения модели параметры, а также определить их оптимальное количество.

После выполнения обозначенных выше пунктов предполагается исследовать область применимости построенной модели защиты, а также провести анализ работоспособности данной модели.

Библиографические ссылки

1. *Hashizume Naoki*, *Momose Fumiyuki*, *Chao Jinhui.* On Implementation of GHS Attack against Elliptic Curve Cryptosystems over Cubic Extension Fields of Odd Characteristics. – 2008.

2. *Brown Daniel R. L.* The Encrypted Elliptic Curve Hash. – 2008.

3. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А. А. Болотов [и др.]. – М. : КомКнига, 2006. – 328 с.

O. O. Karpova, Candidate for a Degree, Perm State Technical University
L. N. Krotov, Doctor of Physical and Mathematical Sciences, Professor, Perm State Technical University
E. L. Krotova, Candidate of Physical and Mathematical Sciences, Perm State Technical University
A. E. Osipovich, Student, Perm State Technical University

Approach to the Construction of Models of Protection of Automated Systems from Unauthorized Access

The main problem of constructing a model of protection of automated systems from unauthorized access are presented. A part of the job for software development required to reach one of the goals is formulated.

Key words: mathematical modeling, automatic control theory, information security.

УДК 65.011.46

M. Jurova, Cand. Sc., Brno University of Technology
E. Chytilova, PhD student, Brno University of Technology
T. Supina, PhD student, Brno University of Technology

THE DEVELOPMENT OF COMPETITIVENESS OF INDUSTRY ENTERPRISES IN CONDITIONS OF EUROPEAN UNION

The current status of industry in European Union and possibilities of its development are considered. The modern trends in optimization of planning and realization of manufacturing are described. In comparing with other countries of European Union we have still a lot of places for improvements, mostly in material and wage savings. The optimization of production tools is still not so popular to bring results in lower costs. Authors focused on modern trends, such as theory of constraint, optimized production technology, advanced planning and scheduling and other.

Key words: industry enterprises, European Union, competitiveness, theory of constraint (TOC), optimized production technology (OPT), just-in-sequence (JIS), single minute exchange of dies (SMED), advanced planning and scheduling (APS), Heuristic Factory Planning Algorithm (HFPA).

Industry is important sector of the national economy. Industry influences in important rate of development and positive routing in individual regions. Industrial production is that part of material transformation, which includes machine process of raw material extraction and obtained agricultural products, conveyances, electronic, pharmaceutical products, plastic and wooden products, etc. Scope of work for industry production isn't coincidence. The share on gross domestic product (hereinafter referred to as GDP) of country speak about significant of this topic.

For example, in Slovakia industrial production hold important place from the point of view inhabitant employment rate, in year 2009 worked in this economy branch 21,04 % working people, what present 497 833 people (in year 2008 it was 24,08 %). The research of ways optimization manufacturing is one of actual themes in current conditions of European business.

Получено 29.06.11