# ОСОБЕННОСТЬ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

УДК

Пацюк И. В., студентка 4 курса
факультета экономической информатики
ХНЭУ им. С. Кузнеца

*Аннотация. В роботе были выявлены источники угрозы информации и определение способов защиты от них. Для обеспечения защиты и конфиденциальности информации в компьютерных системах часто используются криптосистемы с открытым ключом. В частности, их можно использовать для построения математической модели контроля доступа в компьютерной системе.*

*Abstract. The papers identified the sources of threat information and identify ways to protect against them. To ensure the security and privacy of information in computer systems are frequently used public-key cryptosystems. In particular, they can be used to construct a mathematical model of access control in a computer system.*

*Ключевые слова: система защиты информации, безопасность, криптосистема.*

Проблемы обеспечения информационной безопасности предприятия постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего вычислительных систем. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которые должны быть обеспечены: целостность данных; конфиденциальность информации; доступность для всех авторизованных пользователей. Для их реализации имеется ряд методов, которые в целом позволяют обеспечить достаточный уровень информационной безопасности предприятия.

В целом специалисты в области защиты информации предлагают разделять систему безопасности на две части: внутреннюю и внешнюю [1]. Во внутренней части осуществляется, в основном, контроль доступа путем идентификации и аутентификации пользователей при допуске в сеть и при доступе в базу данных. Кроме этого шифруются и идентифицируются данные во время их передачи и хранения. Безопасность во внешней части сети в основном достигается криптографическими средствами.

Впервые криптосистема с открытым ключом на линейных кодах была предложена Р. Мак-Элис в 1978 году которая на сегодняшний день так и остается весомым конкурентом среди других систем [3].

К преимуществам подобных криптосистем можно отнести сравнительно высокую скорость шифрования / расшифровки данных. Кроме того, некоторые из криптосистем на линейных кодах могут быть использованы для одновременного шифрования и помехоустойчивого кодирования данных, или же для одновременного шифрования сообщения и разделения его на части - по схеме разделения секрета.

Разработка криптосистем для таких задач как защита, сохранение целостности и конфиденциальности информации в компьютерных системах передачи данных на сегодняшний день является важным вопросом.

Но в процессе создания таких алгоритмов возникает ряд проблем, они выражены в недостатках обмена данными децентрализованные системы. Высокая надежность таких систем приводит к очень серьезным проблемам связанных с управлением системой и достоверностью распространенной в ней информации и вызывает ряд недостатков: управление системой; информационная соответствие; безопасность; большие затраты на поддержку сети; возникновение большого количества ошибок.

Важным недостатком такой системы также является факт «паразитного подключения». Под этим термином понимают то, что большинство пользователей не открывают доступ к собственным файлам, а лишь пользуются открытыми. Таким образом, превращая систему с децентрализованной архитектурой на клиент-серверную систему. На равных правах с рядом проблем можно определить значительные преимущества: стремительный рост количества абонентов; устойчивость системы по отношению к сбоям; устойчивость в отношении внешних технологических вмешательств; масштабирования системы; балансировки нагрузки; широкой полосой пропуска.

Такие преимущества ставят децентрализованные компьютерные системы на шаг впереди перед другими.

Для построения системы обеспечения информационной безопасности предлагается алгоритм, который содержит следующие этапы:

- построение и анализ математической модели децентрализованной системы;

- построение и анализ криптосистем с открытым ключом; исследование принципов работы децентрализованной системы;
- построение и анализ математической модели контроля доступа к файлам и директориям;
- построение и анализ математической модели контроля доступа к файловой системе.

Проведен анализ возможных уязвимых мест в сетевых системах, позволил определить, что основными источниками является аппаратура, информационный сервер, пароли и среда передачи данных. Если информационный сервер может быть защищен организационными мерами, то среда передачи данных так не защитишь. Отметим, что современная надежная криптографическая система должна удовлетворять следующим требованиям: процедуры шифрования и дешифрования должны быть "прозрачные" для пользователя; дешифрование закрытой информации должно быть максимально затруднено; содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма; надежность криптозащиты не должна зависеть от содержания в секрете самого алгоритма шифрования.

Реально оценить устойчивость крипто алгоритмов невозможно, поскольку большинство из них создателей не желает их раскрывать, ссылаясь на коммерческую тайну, а это не дает возможности провести анализ таких алгоритмов. Не стоит рассчитывать на то, что устойчивость этих алгоритмов выше, чем у тех, которые были опубликованы.

Таким образом, построение системы позволит в целом снизить экономический ущерб, риски, потери информации.

Литература:

1. Галицкий А. В., Рябко С. Д., Шаньган В. Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.: ил.

2. Норткатт С., Новак Д., Маклахлен Д. Обнаружение вторжений в сеть. Издательство "ЛОРИ", 2001, – 384 с.

3. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inform. Theory. V. 31. P. 469-472. 1985.

Научный руководитель к.э.н., доцент, Чаговец Л.А.