СОВРЕМЕННЫЕ ИТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АСУ

Почовян С.М., Габедава О.В.
Грузинский Технический Университет

Резюме

Рассмотрены основные современные информационные технологии обеспечения безопасности информации в автоматизированной информационной системе управления, необходимые для обеспечения эффективного функционирования фирмы. Описаны информационная технология облачных вычислений, системы обнаружения вторжений и система предотвращения вторжений, технология клиент-сервер, основные задачи системы защиты информации для выполнения бизнес-процессов в фирме, а также структура системы автоматизированного управления информационной безопасностью автоматизированной информационной системы управления.

Ключевые слова: АСУ. Информационная система. Защита информации. ИТ. Безопасность.

1. Введение

Для обеспечения эффективности и конкурентоспособности фирмы необходимо обеспечить разработку автоматизированной информационной системы управления, с необходимостью вывода её на уровень современных требований.

Эффективное функционирование фирмы обеспечивается использованием в автоматизированной информационной системы управления современных информационных технологий на основе использования современных методов планирования, контроля и анализа финансово-хозяйственной деятельности, эффективной организации информационного обмена с потребителями информации, с обеспечением защиты информации в коммерческой деятельности фирмы.

2. Основная часть

Для эффективного функционирования фирмы необходимо использовать современнын информационные технологии, применять современные методы использования сети Интернет, включая применение концепции облачных вычислений, создания электронных каталогов услуг всех сервисных служб, а также принятия управленческих решений, с учётом информации внешней среды. Информационная технология облачных вычислений (Cloud computing) позволяет фирме использовать ресурсы Интернета для создания, хранения, представления, обработки и обмена информации, с представлением множества вычислительных услуг и приложений.

Необходимо обеспечить контроль и защиту информации в коммерческой деятельности фирмы, примененять криптографические методы и средства защиты информации, уменьшить риск незаконного вмешательства в процессы функционирования автоматизированнй информационной системы управления, разработать совокупность организационных и технических мер защиты информации для системы защиты автоматизированной информационной системы управления, для устранения угроз безопасности информации. При решении основных задач автоматизированной информационной системы управления должна быть обеспечена доступность ко всей используемой и обрабатываемой в системе информации,

а также их целостность и конфиденциальность, с определением неправомерного копированая, исправления и удаления информации, включая угроз нарушения целостности и подделки электронного документа. Для обнаружения неавторизованного доступа в автоматизированную информационную систему управления через сеть Интернет необходимо использовать системы обнаружения вторжений (Intrusion Detection System): хостовые – ддя отслеживания файлов журналов брандмауэра, веб-сервера и системных журналов, и целостности системных файлов; сетевые – для проверки сетевого трафика на наличие подозрительных шаблонов и обнаружения аномалий. Для компьютерной и сетевой безопасности автоматизированной информационной системы управления необходимо использовать систему предотвращения вторжений (Intrusion Prevention System), в которой система обнаружения вторжений (Intrusion Detection System) связана с брандмауэром, и таким образом система предотвращения вторжений (хостовая, сетевая и распределённая) обнаруживает вторжения и автоматически защищает от них.

Для обеспечения безопасности информации при разработке системы защиты автоматизированной информационной системы управления необходимо учитывать состав, режимы функционирования и функциональные характеристики автоматизированной информационной системы управления, включая программное обеспечение, информационные её взаимосвязи со всеми другими телекоммуникационными сетями и автоматизированными информационными системами управления, с определением объектов защиты, методов управления доступом, типов доступа к информации, правил разграничения доступа, структуры системы защиты автоматизированной информационной системы управления, с определением средств защиты информации.

Должно быть обеспечено оперативное централизованное управление системой защиты информации автоматизированной информационной системы управления, сопровождение функционирования системы защиты, мониторинг за обеспечением уровня защищённости автоматизированной информационной системы управления фирмы, с определением сотрудников фирмы, которые обеспечивают изменения функциональных характеристик автоматизированной информационной системы управления и системы защиты, анализ функционирования системы защиты автоматизированной информационной системы управления, с оперативным устранением недостатков в функционировании системы защиты.

Для защиты коммуникаций автоматизированной информационной системы управления необходимо применить технологию IP-безопасности, которая базируется на протоколе IPSec (IP Security). Данный протокол представляет собой протокол транспортного уровня с защитой данных на основе шифрования, цифровой подписи и алгоритмов кэширования.

Данная технология позволяет осуществлять, при обмене информации между пользователями и компьютерными сетями, защиту информации от перехвата, исправления и копированая [1].

Структура системы автоматизированного управления информационной безопасностью автоматизированной информационной системы управления должна иметь трёхуровневую архитектуру (рис.1).

На первом уровне (уровень сбора информации) происходит сбор, первичная обработка и передача на второй уровень собранной информации по событиям информационной безопасности, а также интеграция с системой физической защиты информации. Средствами SIEM-систем (Security Information and Event Management), либо набором специализированных коннекторов, обеспечивающих сбор необходимой информации, осуществляется сбор информации от систем и средств обеспечения информационной безопасности, системного и специального прикладного программного обеспечения автоматизированной информационной

системы управления, сетевого оборудования, серверов, межсетевых экранов и средств антивирусной защиты.

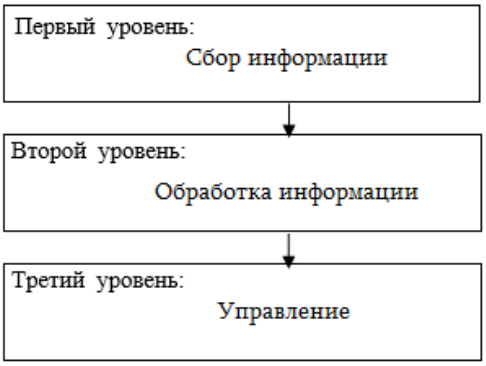

Рис.1. Структура АСУ информационной безопасностью

На втором уровне (уровень обработки информации) осуществляется сбор, анализ и корреляция событий, поступающих от первого уровня. Средствами SIEM-систем (Security Information and Event Management) осуществляется проверка собранной информации на соответствие политике управления инцидентами, обрабатка и корреляция информации, с выделением из множества событий информационной безопасности информации по инцидентам, а также передача полученной информации на третий уровень. На третьем уровне (уровне управления) осуществляется автоматизация процесса управления информационной безопасностью автоматизированной информационной системы управления, и таким образом, данный уровень представляет собой адаптивный интерфейс, который в режиме реального времени управляет инцидентами информационной безопасности, проводит анализ состояния системы защиты, выдаёт отчётную информацию по состоянию информационной безопасности автоматизированной информационной системы управления фирмы.

Разработанная система защиты автоматизированной информационной системы управления обеспечивает управление доступом пользователей к информационным распределённым базам данных и программам, контроль и анализ защищённости информации и угроз безопасности информации и рисков, обнаружение вторжений, антивирусную защиту, контроль Интернет и почтового трафиков, криптографическую защиту информации, целостность и защиту автоматизированной информационной системы управления, включая информационное и программное обеспечения, машинные носители [2]. Таким образом обеспечивается безопасность информации в автоматизированной информационной системе управления, то есть обеспечивается защита от внутренних и внешних угроз.

Процессный подход к разработке новой системы управления обеспечит автоматизацию технологий выполнения бизнес-процессов в фирме. На процедурном уровне фиксируются решения по документообороту, учёту, организации управления, планированию и прогнозированию. С повышением требований к безопасности информации и для уменьшения нагрузки на компьютерную сеть используется современная технология клиент-сервер, которая базируется на реляционных серверах баз данных с передачей по сети лишь изменённой информации. Сотрудники фирмы получают возможность работать с системой на локальных таблицах с привычным для них интерфейсом и получать необходимую информацию от других пользователей по компьютерной сети. Данная технология

обеспечивает равномерное распределение нагрузки на серверные и клиентские узлы и защиту информацционных баз данных от несанкционированного доступа на уровне сервера [1,2].

3. Заключение

Современные информационные технологии обеспечивают эффективность и конкурентоспособность фирмы. Процессный подход позволяет автоматизировать технологии выполнения бизнес-процессов и сократить количество уровней принятия решения в фирме. Для обеспечения безопасности информации необходимо учитывать состав, режимы функционирования и функциональные характеристики автоматизированной информационной системы управления. На основе разработанной системы защиты автоматизированной информационной системы управления обеспечивается доступность ко всей используемой и обрабатываемой информации, с обеспечением их целостности и конфиденциальности.

Литература:

1. С.М. Почовян, Г.Р. Майсурадзе. (2009). Проектирование баз данных. სტუ, საგ.სახლი „ტექნიკური უნივერსიტეტი", თბილისი

2. გაბედავა ო., პოჩოვიანი ს. (2012) სერვერული ტექნოლოგიები. სტუ, საგ.სახლი „ტექნიკური უნივერსიტეტი". თბილისი.

INFORMATION SECURITY MODERN IT FOR AUTOMATED MANAGEMENT INFORMATION SYSTEMS

Pochovyan Simon, Gabedava Omar
Georgian Technology University

Summary

The basic modern information technology security information in an automated information management system required for the effective functioning of the company. Describes information technology cloud computing, intrusion detection systems and intrusion prevention system, client-server technology, the main task of protecting information for the execution of business processes in the company, as well as the structure of the automated control system of information security of automated information management system.

ინფორმაციის უსაფრთხოების უზრუნველყოფის თანამედროვე ტექნოლოგიები მართვის ავტომატიზებულ სისტემებში

სიმონ პოჩოვიანი, ომარ გაბედავა
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია მართვის ავტომატიზებულ სისტემებში ინფორმაციის უსაფრთხოების უზრუნველყოფის თანამედროვე ინფორმაციული ტექნოლოგიები., აუცილებელი ფირმის ეფექტური ფუნქციონირებისათვის. აღწერილია ღრუბლოვანი გამოთვლების ინფორმაციული ტექნოლოგია, „შეჭრის" აღმოჩენის სისტემები და მათი აღკვეთის სისტემა, კლიენტ-სერვერული ტექნოლოგია, ფირმაში ბიზნეს-პროცესების შესრულებისათვის ინფორმაციის დაცვის სისტემის ძირითადი ამოცანები, აგრეთვე, მართვის ავტომატიზებული სისტემის ინფორმაციული უსაფრთხოების, მართვის ავტომატიზებული სისტემის სტრუქტურა.