

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Семён Почовян
Грузинский Технический Университет

Резюме

Рассмотрены вопросы разработки и внедрения автоматизированной информационной системы в организации, а также проблемы их безопасности. Описаны основные вопросы обеспечения информационной безопасности, система защиты информации, основные работы построения система защиты информации, основные методы защиты информации, технические и программные средства защиты информации, основные условия построения система защиты информации, для эффективного использования информационных технологий и автоматизированной информационной системы.

Ключевые слова: Автоматизированная информационная система. Субъекты информационных отношений. Информационная безопасность. Система защиты информации.

1. Введение

Разработка и внедрение автоматизированной информационной системы обеспечивает эффективное функционирование организации и необходимое качество управления за счёт использования достоверных данных информационной бвзы данных и выработки управленческих решений.

Информационные системы управления классифицируют а зависимости от видов процессов управления, уровня управления, степени автоматизации управления, сферы функционирования и т.д. Автоматизированная информационная система представляет собой совокупности информации, экономико-математических методов и моделей, технологических, технических, программных средств и специалистов, предназначенную для хранения, обработки информации и выдачи информации в интересах достижения поставленной цели и принятия управленческих решений. Цель и характер деятельности организации определяют её информационную систему и автоматизацию информационной технологии. Задачей информационной системы является информационное обеспечение предметной деятельности организации. Результатом применения современных информационных технологий является предоставление пользователям необходимых данных в виде информационных услуг [4].

В современных условиях информационный менеджмент опирается на использование информационных технологий и персональных компьютеров. Внедрение и распространение информационных технологий и персональных компьютеров делает их уязвимыми к деструктивным воздействиям. Высокая степень автоматизации порождает снижение информационной безопасности. Возникает проблема безопасности разработки и использования автоматизированной информационной системы в организации.

2. Основная часть

Для обеспечения информационной безопасности субъектов информационных отношений (владельцев, поставщиков и потребителей информации) автоматизированных информационных систем, при выполнении экономических и производственно-хозяйственных задач, необходимо обеспечить: конфиденциальность, целостность и достоверность

информации; контроль и управление процессами обработки, хранения и передачи информации; определение прав субъектов информационных отношений [3-4].

Под информационной безопасностью понимают состояние (уровень) защищённости информационных ресурсов (информационных систем и информационных объектов) от негативных воздействий (случайных и преднамеренных), которые могут нанести ущерб информации и средствам её обработки, хранения и передачи, а также субъектам информационных отношений. Под информационной безопасностью понимают совокупность методов, средств и процессов (процедур), обеспечивающих эффективное функционирование технической инфраструктуры информационных систем, а также обрабатывающей и хранящейся информации. Обеспечение информационной безопасности должна обеспечить удовлетворение прав субъектов информационных отношений. Информационная безопасность связана с рисками для информационных ресурсов, то есть возможностью нанесения ущерба информационным ресурсам и снижения уровня их защищённости. Информационными ресурсами организаций являются информационные базы данных различного назначения, то есть все виды информации, необходимые и доступные субъектам информационных отношений для эффективного выполнения функциональных задач организаций. На основе баз данных в организациях осуществляется: автоматизированная регистрация, ввод, накопление, хранение и обработка информации, автоматизированные расчёты, информационное обслуживание субъектов информационных отношений и т.д. Информационные базы данных характеризуются распределённой обработкой данных и наличием хранилищем данных с интеллектуальными технологиями поддержки принятия решений [1-4].

Информационная безопасность является основной частью современных информационных технологий, мультимедийных технологий. Система информационной безопасности должна противостоять внешним и внутренним атакам нарушения составляющих информационной безопасности – конфиденциальности, целостности и доступности информации [3-4].

Для обеспечения нормального функционирования субъектов информационных отношений необходимо организовать средства обеспечения безопасности информации от модификации, утечки и утраты, несанкционированного использования и модификации информационных ресурсов, распространения вирусов и вредоносных программ, вывода из строя аппаратных и программных средств обработки, хранения и передачи информации. Для этого необходимо обеспечить защиту всех компонентов информационных технологий и автоматизированных систем: информации, программных и технических средств. Для этого необходимо построить систему защиты информации, включающую следующие работы: определение угроз безопасности информации (недоступность информационных ресурсов, разрушение (потеря) информации, вскрытие шифров криптозащиты информации, информационные угрозы и риски при использовании облачных сервисов, нарушение конфиденциальности информации и т.д.), определение каналов несанкционированного доступа и утечки информации, определение методов, механизмов и средств защиты информации. Таким образом система защиты информации должна обеспечивать: выполнение основных функций автоматизированной информационной системы обработки данных; соблюдение правил разграничения доступа к информации, включая к конфиденциальной информации; учёт случаев нарушения безопасности информации в автоматизированной системе; организацию работ по защите информации и управления; учёт случаев нарушения безопасности информации в АСУ [3-4].

К методам защиты информации относятся:

- Управление доступом, с идентификацией ресурса системы и субъектов информационных отношений;

- Препятствия к техническим средствам;

Маскировка путём криптографического закрытия информации. Кроме того, применение криптографических методов позволяет решать задачи других направлений обеспечения безопасности, например обнаружение несанкционированного изменения данных, автоматическое восстановление от угроз безопасности информации, попытки установления несанкционированных соединений, отказ в обслуживании, и т.д.;

Регламентация и принуждение, обеспечивающие субъектам информационных отношений условия и правила обработки, хранения, передачи и использования защищаемой информации.

К основным средствам защиты информации, необходимым для создания механизма обеспечения безопасности, относятся:

Технические средства (аппаратные, например, системы разграничения доступа к информации на основании паролей, записи кодов и т.д.; физические средства, реализующие в виде автономных систем и устройств);

Программные средства, представляющие программное обеспечение (например: механизмы контроля доступа; механизмы управления маршрутизацией; программы идентификации; программы регулирования работ (функциональных задач, баз данных, субъектов информационных отношений, технических средств, и т.д.) антивирусные программы; механизм шифрования (криптография); механизм цифровой подписи; механизмы обеспечения целостности данных, программы архивации и т.д.) [1-2].

Таким образом, система защиты информации представляет собой комплекс мероприятий, направленных на обеспечение информационной безопасности. Необходимо учитывать следующие условия построения системы защиты информации: 1) построение средств защиты информации необходимо осуществлять в процессе функционирования организации и изменений внешних условий; 2) алгоритм и механизм защиты информации должен обеспечить субъектов информационных отношений необходимой информацией для выполнения экономических и производственно-хозяйственных задач; 3) построенная система защиты информации должна быть эффективной для определения угроз безопасности информационных технологий, информации, а также облачных приложений и сервисов

3. Заключение

Для эффективной работы всех субъектов информационных отношений (владельцев, поставщиков и потребителей информации) и их организаций, в процессе принятия управленческих решений в организации, обеспечения безопасности обработки, хранения и передачи информации в системе, – защита информации, программных и технических средств информационных технологий и автоматизированных информационных систем представляет собой непрерывный целенаправленный процесс, с установлением необходимых средств защиты информации.

Необходимо оперативно внедрять новые информационные технологии и развивать инновационный процесс. Информационные технологии в организациях используются при составлении документации, визуализации производственного процесса, мониторинге и контроле, а также принятии управленческих решений. Для эффективного использования информационных технологий в управленческих и производственных процессах организации средства защиты информации должны выполнять защитные функции, согласно целенаправленной деятельности субъектов информационных отношений, а также по заранее предусмотренным процедурам без участия субъектов информационных отношений.

ლიტერატურა - References – Литература:

1. Почовян С.М., Майсурадзе Г.Р. (2009). Проектирование баз данных. სტუ, „ტექნიკური უნივერსიტეტი“. თბილისი.
2. Габедава О.В., Почовян С.М. (2010). Серверные технологии. სტუ, „ტექნიკური უნივერსიტეტი“. თბილისი.
3. Почовян С.М., Габედავა О.В., Габედავა Н.О. (2014). Использование современных автоматизированных информационных технологий в фирмах. სტუ-ს შრ.კრ. „მართვის ავტომატიზებული სისტემები“, №1(17), თბილისი. გვ. 76-79.
4. Почовян С.М (2016). Использование информационных технологий в процессах принятия управленческих решений. სტუ-ს შრ.კრ. „მართვის ავტომატიზებული სისტემები“, №2(22), თბილისი. გვ. 139-142.

ავტომატიზებული საინფორმაციო სისტემების ინფორმაციის დაცვა

სიმონ პოხოვიანი

საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ავტომატიზებული საინფორმაციო სისტემის განვითარების და განხორციელების საკითხები ორგანიზაციაში, ასევე მათი უსაფრთხოების პრობლემები. აღწერილია საინფორმაციო ტექნოლოგიების და ავტომატიზებული საინფორმაციო სისტემის ეფექტური გამოყენების ინფორმაციული უსაფრთხოების უზრუნველყოფის ძირითადი საკითხები, ინფორმაციის დაცვის სისტემა, ინფორმაციის დაცვის სისტემის აგების ძირითადი სამუშაოები, ინფორმაციის დაცვის ძირითადი მეთოდები, ინფორმაციის დაცვის ტექნიკური და პროგრამული საშუალებები, ინფორმაციის დაცვის სისტემის აგების ძირითადი პირობები.

INFORMATION SECURITE IN THE AUTOMATED INFORMATION SYSTEMS

Pochovyan Simon

Georgian Technology University

Summary

Questions development and introductions of the automated information system in the organization, and also problems of their safety are considered. The main questions of ensuring information security, system of information security, the main works of construction system of information security, the main methods of information security, technical and software of information security, the main conditions of construction system of information security, for effective use of informational technologies and the automated information system are described.