Экономическая и информационная безопасность: проблемы обеспечения в российской экономике

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Никитина Дарья Сергеевна
Финансовый университет, Москва, Россия
E-mail: sutofa@yandex.ru

В современном мире очень остро встает проблема защиты информации, обеспечение ее безопасности и сохранение коммерческой тайны.

Современные автоматизированные информационные технологии обладают следующими признаками:

1) Различной степенью конфиденциальности содержащейся на носителе информации

2) Острой необходимости в криптографической защите информации.

3) Потребностью в обязательном учете и регистрации всех попыток несанкционированного доступа.

4) Необходимым обеспечением целостности ПО и информации.

5) Наличием физической охраны средств вычислительной техники.

К сожалению, обеспечить информационную безопасность без существенной организационной и финансовой поддержки в современном мире просто невозможно, ведь самая лучшая защита является самой дорогой.

Очень важное место в обеспечении безопасности информационных данных занимает непосредственная охрана объекта.

При создании базовой системы защиты информации необходимо учитывать следующие принципы. Первым из них является комплексный подход к устройству систем защиты, призванный обеспечить наиболее разумное и оптимальное сочетание организационных и программных методов и средств защиты. Очень важно для нахождения оптимального сочетания между программными и организационными мерами защиты учитывать зарубежный опыт в создании успешно функционирующих систем защиты.

Вторым принципом обеспечения безопасности систем информации является разделение и минимизация полномочий, другими словами, передача пользователям строго определенного минимума полномочий, необходимых для выполнения ими своих непосредственных обязанностей.

Третьим принципом является полнота контроля и регистрации попыток несанкционированного доступа. Иначе говоря, этот принцип подразумевает установление идентичности пользователей и строгое протоколирование их действий. Это необходимо для того, чтобы возможно было провести расследование и установить причины краха системы безопасности, если таковой произойдет. Также это подразумевает невозможность выполнения любого действия по обработке или удалению информации в АИТ без предварительной регистрации данной операции.

Четвертым принципом является обеспечение надежности системы защиты, что подразумевает невозможность изменения уровня защиты информации, его снижение при возникновении тех или иных сбоев в системе, вероятно вызванных преднамеренными действиями нарушителя или же совершенно непреднамеренными, случайными действиями пользователей.

Пятым принципом является обеспечение контроля за функционированием защитных систем. Это означает создание определенных методов и средств контроля за работоспособностью защитных механизмов системы.

Экономическую целесообразность использования защитных систем нельзя не отнести к базовым принципам обеспечения информационной защиты и безопасности. Смысл этого принципа заключается в том, что стоимость разработки и последующей эксплуатации системы защиты не должна превышать стоимость возможного ущерба, который может нанести объекту эксплуатация АИТ без системы информационной защиты.

Механизмы криптографии используются в современном мире для реализации мер безопасности. Их сущность заключается в следующем: для предотвращения получения несанкционированного доступа к передаваемым данным, последние зашифровываются, преобразовываясь в шифрограмму. Когда же тот, чей доступ к данным санкционирован, получает данные, он должен дешифровать или же раскрыть их путем обратного преобразования криптограммы, что позволяет ему получить исходные данные, отправленный ему их первоначальным обладателем. Кроме того, для обмена зашифрованными данными необходимо, чтобы и отправитель, и получатель этих данных знали и хранили в тайне верную ключевую установку.

Для преобразования данных в криптограммы используется специальный алгоритм, чье действие запускается шифрующим ключом, способным создавать различные шифрованные сообщения.

Таким образом, степень секретности ключа определяет уровень безопасности передачи данных. Для увеличения безопасности следует пользоваться новейшими технологиями и достижениями иностранных специалистов, следить за новейшими открытиями и не стараться чрезмерно сэкономить средства на безопасности данных, полагая обеспечение безопасности задачей не первостепенной, почти неважной, а ведь это может привести к поистине ужасающим для бизнеса последствиям, утере важнейших данных и потере множества деловых связей. К сожалению, далеко не все современные бизнесмены понимают это, стремясь сэкономить на безопасности собственных данных, что, в результате, приводит к еще большим затратам и, в конце концов, все же увеличению уровня безопасности передачи данных. При соблюдении всех принципов и верном выборе системы безопасности пользователь может быть спокоен за свои данные.

Источники и литература

1) Титоренко Г.А. Автоматизированные информационные технологии в экономике. М.: ЮНИТИ, 2008.

2) Тихомиров В.П., Хорошилов А.В. Введение в информационный выбор. М.: Финансы и статистика, 2009.

3) Глазьев В.П. Операционные технологии межбанковского финансового рынка. М.: ЮНИТИ, 2009.

4) Лопатин В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000. - 428 с

5) Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. - 544 с