УДК 004.56

Лузин Алексей Иванович

аспирант кафедры антикризисного управления, налогов и налогообложения Кубанского государственного университета a2004555@rambler.ru

ИННОВАЦИОННЫЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ

Аннотация:
В статье рассматриваются основные способы и направления обеспечения инновационного процесса на предприятиях, взаимосвязь экономической и информационной безопасности. Информационная безопасность – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Ключевые слова:
информация, безопасность, инновации, экономическая стабильность, развитие, устойчивость к взлому, рациональность, уязвимость.

Luzin Alexey Ivanovich

post-graduate student of the chair of crisis management, taxes and taxation, Kuban State University a2004555@rambler.ru

INNOVATIVE WAYS TO ENSURE INFORMATION SECURITY IN ENTERPRISES

The summary:
The article deals with basic methods and guidelines for ensuring the innovation process in enterprises, the relationship of economic and information security. Information security is such the state of the system, in which, on one hand, it is able to withstand the destabilizing impact of external and internal information threats, and on another – its operation does not create threats to the information elements of the system and the external environment.

Keywords:
information security, innovation, economic stability, development, resistance to cracking, rationality, vulnerability.

Безопасность определяется как состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – ее функционирование не создает угроз для элементов самой системы и внешней среды. Доктрина информационной безопасности Российской федерации определяет информационную безопасность как состояние защищенности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз.

Для решения проблем информационной безопасности необходимо достигнуть решения трех составляющих проблем:

первая – защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;

вторая – защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;

третья – защита внешней среды от информационных угроз со стороны рассматриваемой системы.

Государство в глазах общества представляет, прежде всего, его интересы. При этом личная, общественная и экономическая безопасность практически обеспечивается государством. Оно же должно обеспечивать соблюдение законных прав граждан и организаций на информацию, предотвращать неправомерное ограничение доступа к документам и сведениям, содержащим важную для граждан и организаций информацию, и другие действия, которые должны рассматриваться как угроза информационной безопасности (ИБ).

Инновационные автоматизированные информационные технологии, применяемые при управлении различных сфер деятельности предприятий и организаций, базируются на применении компьютерных сетей от локальных до глобальных и обладают следующими основными признаками ИБ:

– наличие информации различной степени конфиденциальности;

– необходимость криптографической защиты процессов пользования информацией различной степени конфиденциальности при передаче данных;

– иерархичность полномочий субъектов доступа и программ и автоматизированному рабочему месту (АРМ), файл-серверам, каналам связи и информации системы; необходимость оперативного изменения этих полномочий;

– организация обработки экономической информации в диалоговом режиме, режиме разделения времени между пользователями и режиме реального времени;

– обязательное управление экономическими потоками информации и обеспечение экономической безопасности как в локальных сетях, так и при их передаче по каналам связи на далекие расстояния;

– необходимость применения инновационных технологий для регистрации и учета попыток несанкционированного доступа, событий в системе и документов, выводимых на печать.

Организационные мероприятия и процедуры, используемые для решения проблемы безопасности переработки информации, необходимо решать на всех этапах проектирования и в процессе эксплуатации автоматизированных информационных технологий (АИТ).

Без надлежащей организационной поддержки программно-технических средств защиты переработки информации от несанкционированного доступа и точного выполнения предусмотренных проектной документацией процедур в должной мере не решить проблему обеспечения безопасности переработки информации, какими бы совершенными эти программно-технические средства не были.

Системы защиты процессов переработки экономической информации в АИТ необходимо строить на следующих принципах:

– комплексный подход к построению системы защиты при ведущей роли организационных мероприятий, означающий оптимальное сочетание программно-аппаратных средств и организационно-экономических и подтвержденный практикой создания отечественных и зарубежных систем защиты;

– разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки;

– обеспечение надежности системы защиты за счет использования последних инновационных разработок;

– экономическая целесообразность использования системы защиты, выражающаяся в том, что стоимость разработки и эксплуатации систем защиты обработки информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации АИТ без системы защиты.

Средства обеспечения безопасности процессов переработки информации, используемые для создания механизма зашиты, подразделяются на формальные (выполняют защитные функции по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Если рассматривать неформальные средства защиты, можно выделить:

– организационные, представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты обработки информации;

– законодательные, которые определяются законодательными актами страны, регламентирующими правила пользования, обработки и передачи информации ограниченного доступа и устанавливающими меры ответственности за нарушение этих правил;

– морально-этические, которые реализуются в виде всевозможных норм, сложившихся традиционно или складывающихся по мере распространения вычислительной техники и средств связи в обществе.

Также необходимо использование инновационных механизмов контроля доступа, осуществляющего проверку полномочий объектов АИТ (программ и пользователей) на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке. Механизмы обеспечения целостности данных применяются как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но недостаточным условием целостности потока. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

Аутентификация может быть односторонней и взаимной. В первом случае один из взаимодействующих объектов проверяет подлинность другого, тогда как во втором случае проверка является взаимной.

Механизмы постановки трафика, называемые также механизмами заполнения текста, используются для реализации засекречивания потока данных. Они основываются на генерации объектами АИТ фиктивных блоков, их шифровании и организации передачи по каналам сети. Этим нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по скомпрометированным (небезопасным) физически ненадежным каналам.

Механизмы арбитража, или освидетельствования, обеспечивают подтверждение характеристик данных, передаваемых между объектами АИТ, третьей стороной (арбитром). Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.

Таким образом, можно сделать вывод, что информационная безопасность является неотъемлемой частью жизни человека в различных сферах. При этом необходимо уделять внимание экономической безопасности и учитывать последние инновационные разработки, а также применять не только технические, механические, программные и аппаратные средства доступа, но и брать во внимание организационный аспект и снижение затрат на разработку систем защиты.