Комплексный анализ проекта обеспечения информационной безопасности

в коммуникационных системах

Информационная безопасность с точки зрения государства и права

В статье описывается опыт по обеспечению информационной безопасности операционных систем и систем управления базами данных организационных сложных иерархических структур. Приводится проект комплексной системы обеспечения информационной безопасности, базирующийся на иерархическом подходе к моделированию сложных систем управления.

Сергей Ковалев, профессор

В настоящее время в областях информационных технологий (ИТ) стоят на первом месте вопросы создания и развития нормативной базы в области информационной безопасности, а также необходимость проведения комплекса работ, направленных на развитие стандартизации и сертификации в области информационной безопасности (ИБ).

Стандарты, определяющие требования по информационной безопасности и являющиеся основой нормативно-правовой базы, важны для всех субъектов отношений в этой области, в первую очередь для тех организаций и предприятий, которые заинтересованы в защите своих информационных ресурсов. Руководству и службам безопасности предприятий следует четко представлять себе, каким требованиям, в зависимости от условий функционирования, должны соответствовать их информационные системы (ИС). Разработчики информационных технологий и информационных систем должны руководствоваться стандартами для обеспечения безопасности своих разработок [1–4].

Любой человек, работающий в сфере ИТ, понимает необходимость обеспечения безопасности операционных систем (ОС). Необходимость наличия встроенных средств защиты на этом уровне не вызывает сомнений. Операционная система обеспечивает защиту механизмов прикладного уровня от неправильного использования, обхода или навязывания ложной информации. Если она не сможет удовлетворить этим требованиям, появятся уязвимости в масштабах всей системы.

Одной из задач ИС является хранение и обработка данных. Для ее решения были предприняты усилия, которые привели к появлению специализированного программного обеспечения — систем управления базами данных (database management systems, СУБД). СУБД позволяют структурировать, систематизировать и организовывать данные для их компьютерного хранения и обработки. Невозможно представить себе деятельность современного предприятия или учреждения без использования профессиональных систем управления базами данных. Несомненно, они составляют фундамент информационной деятельности во всех сферах — начиная с производства и заканчивая финансами и телекоммуникациями. В этом смысле ОС и СУБД похожи друг на друга.

Основу правового регулирования в области обеспечения ИБ операционных систем и систем управления базами данных, где обрабатывается конфиденциальная информация, составляют принятые законы и нормативные акты Российской Федерации. Одним из таких документов является «Доктрина информационной безопасности Российской Федерации», которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ РФ [1]. Доктрина служит основой для формирования государственной политики в области обеспечения ИБ РФ и развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

Интересы личности в информационной сфере заключаются в реализации конституционных

Таблица 1. Виды угроз ИБ РФ

Правовые	• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России; • нерациональное, чрезмерное ограничение доступа к общественно необходимой информации; • нарушение конституционных прав и свобод человека и гражданина в области массовой информации; • угрозы информационному обеспечению государственной политики Российской Федерации; • угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов; • угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России; • противоправные сбор и использование информации.
Технологические	• нарушения технологии обработки информации; • внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; • разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации; • уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи; • воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации; • компрометация ключей и средств криптографической защиты информации.
Организационно-экономические	• утечка информации по техническим каналам; • внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности; • уничтожение, повреждение, разрушение или хищение машинных и других носителей информации; • перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации; • несанкционированный доступ к информации, находящейся в банках и базах данных; • нарушение законных ограничений на распространение информации.

прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность. Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

По своей общей направленности угрозы ИБ РФ подразделяются на правовые; технологические; организационно-экономические (табл. 1). Общие методы обеспечения ИБ РФ — организационно-технические, правовые, организационно-экономические, программно-технические и экономические (табл. 2).

Наиболее важными объектами обеспечения ИБ РФ в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- научно-технические кадры и система их подготовки.

К числу основных внешних угроз ИБ РФ в области науки и техники следует отнести стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах.

К основным внутренним угрозам ИБ РФ в области науки и техники относятся:

Таблица 2. Методы обеспечения ИБ РФ

Организационно-технические	• разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения; • создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи; • выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации.
Правовые	• защита прав граждан на владение, распоряжение и управление принадлежащей им информацией; защита конституционных прав граждан на тайну переписки, переговоров, личную тайну; • контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации, разработка комплекса нормативно-правовых актов и положений, регламентирующих информационные отношения в обществе, разработка руководящих и нормативно-методических документов по обеспечению ИБ.
Организационно-экономические	• лицензирование отдельных видов деятельности, сертификация систем и средств защиты по требованиям информационной безопасности, стандартизация способов и средств защиты информации, контроль (надзор).
Программно-технические	• предотвращение утечки обрабатываемой информации, предотвращение специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, выявление программных или аппаратных закладных устройств, исключение перехвата информации техническими средствами.
Экономические методы	• защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения; защита прав предпринимателей при осуществлении ими коммерческой деятельности.

- сохраняющаяся сложная экономическая ситуация в России, ведущая к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;
- серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;
- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам ИБ РФ в области науки и техники — это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники.

Литература

1. ISO/IEC 17799. Управление информационной безопасностью. Практические правила.
2. Безопасность информационных технологий — Операционные системы — Базовый профиль защиты (проект). Центр безопасности информации. 2003.
3. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
4. ЕСПД ГОСТ 19102-77. «Требования к планированию проектных работ по разработке программного обеспечения».
5. Ковалев С. В. Расчетно-математическая модель управления рисками экономической безопасности проектов развития сложных систем // Проблемы управления безопасностью сложных систем: Труды XVII Международной конференции. М.: РГГУ. 2009.
6. Ковалев С. В. Модель обеспечения защиты информации предприятия на основе принципов риск-контроллинга // Информационная экономика: институциональные проблемы. Материалы Девятых Друкеровских чтений. М: Доброе слово. 2009.
7. Ковалев С. В. Методология информационной безопасности сложных систем на основе системы управления промышленными рисками // Проблемы управления безопасностью сложных систем: Труды XVII Международной конференции. М.: РГГУ. 2009.
8. Ковалев С. В. Методология разработки и применения информационных технологий поддержки жизненного цикла наукоемкой продукции // Информационные технологии моделирования и управления. 2009. № 5(57).