А. А. Малюк

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Москва
Горячая линия – Телеком
2012

Электронный архив библиотеки МГТУ им. Н.Э. Баумана

УДК 004.056
ББК 32.973-018.2
М21

Р е ц е н з е н т ы: доктор физ.-мат. наук, профессор *Г. О. Крылов*, доктор техн. наук, профессор *М. П. Сычев*, доктор техн. наук, профессор *А. А. Тарасов.*

Малюк А. А.

М21 Теория защиты информации. – М.: Горячая линия–Телеком, 2012. – 184 с., ил.

ISBN 978-5-9912-0246-6.

В книге предпринята попытка ответить на объективные потребности формирования концептуальных и методологических основ обеспечения информационной безопасности в процессе развития информационного общества. В ней изложены основы теории защиты информации, объединяющие широкий спектр проблем, связанных с обеспечением информационной безопасности в процессе генерирования, обработки, хранения и передачи информации в автоматизированных системах и на объектах информатизации. Анализируются различные подходы к моделированию систем и процессов защиты информации в условиях неполноты и недостоверности исходных данных. Особое внимание уделено эвристической составляющей процесса поиска наиболее рациональных решений в различных ситуациях защиты информации.

Для специалистов в области обеспечения информационной безопасности, будет полезна студентам и аспирантам высших учебных заведений, слушателям курсов повышения квалификации.

ББК 32.973-018.2

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

Малюк Анатолий Александрович

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника В. Г. Ситникова

Подписано в печать 20.04.12. Формат 60×90/16. Усл. печ. л. 11,5. Тираж 500 экз. (1 завод – 250 экз.)

ISBN 978-5-9912-0246-6

ВВЕДЕНИЕ

Интенсивное развитие и использование современных информационных технологий привели в настоящее время к серьезным качественным изменениям в экономической, социально-политической и духовной сферах общественной жизни. Человечество фактически переживает этап формирования нового информационного общества. Феномен резко возрастающего влияния информационно-коммуникационных технологий на формирование общества XXI века был отмечен в Окинавской Хартии глобального информационного общества, принятой лидерами «восьмерки» 22 июля 2000 г.

Утвержденная в 2008 году Стратегия развития информационного общества в России так характеризует его отличительные черты:

- существенный рост доли в валовом внутреннем продукте отраслей экономики, связанных с производством знаний, с созданием и внедрением наукоемких, в том числе информационных, технологий, других продуктов интеллектуальной деятельности, с оказанием услуг в области информатизации, образования, связи, а также поиска, передачи, получения и распространения информации;
- радикальное ускорение технического прогресса, превращение научных знаний в реальный фактор производства, повышения качества жизни человека и общества;
- участие значительной части трудоспособного населения в производственной деятельности, связанной с созданием и использованием информационных технологий, информации и знаний;
- глобализация экономической, политической и духовной сфер жизни общества.

В этих условиях на передний план экономического и социального развития выходят проблемы совершенствования систем информационного обеспечения всех сфер деятельности общества. Их решению в последние годы посвящаются интенсивные и крупномасштабные исследования и разработки [1].

Вместе с тем, развитие информационного общества, помимо расширения созидательных возможностей, приводит и к росту угроз национальной безопасности, связанных с нарушением установленных режимов использования информационных и коммуникацион-

ных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также с использованием возможностей современных информационных технологий для осуществления враждебных, террористических и других преступных действий [2]. В связи с этим особую остроту сегодня приобретает проблема обеспечения информационной безопасности и, прежде всего, надежной защиты информации (предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования).

Вообще говоря, проблема защиты информации, имея многовековую историю, приобрела самостоятельную актуальность только во второй половине XX века, которая характеризуется бурным развитием средств вычислительной техники. Причем особая острота проблемы была связана с тем, что указанные средства стали применяться и для обработки закрытой информации. В связи с этим и по сей день нередко проблему защиты информации сводят к защите только секретной информации, хотя, как сегодня стало ясно всем, это составляет лишь одну из частей гораздо более общей задачи обеспечения целостности, доступности и конфиденциальности информации и защиты жизненно важных интересов личности, общества и государства в информационной сфере.

Сегодня мы можем констатировать, что в процессе своего развития мировая «информационная» цивилизация пришла к формированию самостоятельного научно-технического направления «Информационная безопасность» и созданию системы подготовки профессиональных специалистов по защите информации. Иными словами, в настоящее время мы фактически имеем дело с новой важной сферой деятельности, основными задачами которой являются:

- организация практических работ по защите информации и управление ими на общегосударственном, региональном и объектовом уровнях;
- проведение научных исследований и разработок всех аспектов рассматриваемой проблемы;
- разработка, производство и распространение средств защиты;
- подготовка кадров в области защиты информации.

Рассматривая общее содержание перечисленных задач, мы можем отметить, что в плане организации работ по защите информации в большинстве стран к настоящему времени на государственном уровне созданы достаточно стройные и эффективные системы управляющих органов. В Российской Федерации, например, основу

этой системы составляют такие государственные структуры, как Совет Безопасности, Федеральная служба безопасности, Федеральная служба по техническому и экспортному контролю, Министерство внутренних дел и др.

На уровне объектов информатизации (предприятия и компании различных форм собственности, учреждения, другие организации) работа по защите информации организуется штатными службами защиты, состав и численность которых определяются объемом соответствующих задач. Как показывает анализ деятельности данных служб, на сегодня они решают свои задачи более или менее эффективно. Однако изменения в понимании существа проблемы защиты информации, подходах, методах и средствах ее решения, которые связаны с активным формированием информационного общества, предопределяют необходимость существенной корректировки как организации, так и содержания их деятельности. В частности, расширение рамок комплексности защиты требует укомплектования соответствующих служб кадрами высококвалифицированных специалистов по техническим, организационным, правовым и гуманитарным аспектам защиты информации. Непрерывный рост арсенала предлагаемых на рынке средств защиты, способов и методов их применения требует оптимального их комплексирования (как по целям, так и по видам), а также организации оптимального управления ими. При этом особенностью проблемы защиты информации является то, что ее решение должно осуществляться в условиях неопределенности, а зачастую и невозможности прогнозирования проявления отдельных дестабилизирующих факторов.

Кроме того, непрерывный рост количества объектов информатизации, нуждающихся в защите информации, но не имеющих возможностей содержать собственную полноценную службу защиты, делает все более актуальной задачу развития аутсорсинга в сфере обеспечения информационной безопасности и создания для этих целей специализированных центров защиты информации. Создание сети таких центров представляется одним из основных способов организационного решения проблемы защиты информации на региональном уровне.

Анализируя доступные нам результаты научных исследований и разработок в области защиты информации, мы можем констатировать, что до последнего времени данные разработки в основном были направлены на развитие технических средств защиты (физических, программно-аппаратных, криптографических). Современный период развития информатизации общества, как это уже отме-

ОГЛАВЛЕНИЕ