Оглавление

Введение

Кто владеет информацией, тот владеет миром.

У. Черчилль

На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первостепенное значение. На смену им приходит новый ресурс, единственный не убывающий, а растущий со временем -- информационный.

Информационные технологии (ИТ) все глубже проникают во многие сферы жизни общества. Информация стала товаром, который можно приобрести, продать, обменять. При этом стоимость информации часто в сотни раз превосходит стоимость компьютерной системы (КС), в которой она хранится и обрабатывается. Этот процесс становится настолько масштабным, что затрагивает жизненные интересы государства, в том числе и в области информационной безопасности.

Современная информационная система (ИС) представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Автоматизированные системы управления (АСУ) широко применяются в атомной, нефтегазоперерабатывающей, химической промышленности, на транспорте, в навигационных системах, системах управления государством и других областях. Практически каждый компонент автоматизированной системы (АС) может подвергнуться внешнему воздействию или выйти из строя.

Таким образом, в настоящее время от степени защищенности информационных технологий зависит благополучие, а порой и жизнь многих людей. Вывод из строя автоматизированных систем может повлечь сбои технологического цикла предприятия, систем управления и сопровождения транспорта и, как следствие, привести к авариям и катастрофам с гибелью населения. Нарушение в информационных процессах может повлечь за собой экономический, экологический или военный кризис. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

Наряду с этим важное значение приобретает зашита национальных информационных ресурсов, обусловленная расширением доступа к ним через открытые информационные сети типа Интернет. Экспоненциально увеличивается число компьютерных преступлений.

Несмотря на то что современные операционные системы (ОС), такие как Windows, Linux или МСВС, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами. К наиболее уязвимым местам, через которые обычно пытаются проникнуть злоумышленники, относятся открытые системы, системы, поддерживающие технологию подключения периферийных устройств в режиме plug-and-play, средства централизованной удаленной поддержки, коммутируемые канаты удаленного доступа и недостаточно надежные технологии шифрования.

В результате возникает проблема защиты информации в автоматизированных системах, которая является одной из основных составляющих обеспечения безопасности информации.

Особая актуальность задачи обеспечения информационной безопасности (ИБ) компьютерных систем в Российской Федерации на современном этапе отражена в таких основополагающих государственных документах, как Федеральный закон РФ "О безопасности", "Стратегия национальной безопасности РФ до 2020 года" и "Доктрина

информационной безопасности РФ". В них отмечается, что именно информационная инфраструктура общества -- первая мишень информационного терроризма.

Не стоит думать, что ввиду унаследованной информационной замкнутости, определенной технологической отсталости Россия менее уязвима, чем другие государства, -- скорее наоборот. Как раз высокая степень централизации структур государственного управления российской экономикой может привести к гибельным последствиям в результате информационной агрессии или террористических действий.

Конечно, российские спецслужбы располагают необходимыми средствами и известным опытом предотвращения перехвата, утечек, искажений, уничтожения информации в информационных и телекоммуникационных сетях и системах общегосударственного назначения. Но темпы совершенствования информационного оружия (как и любого вида атакующего вооружения) превышают темпы развития технологий зашиты. Вот почему задача нейтрализации информационного оружия, парирования угрозы его применения должна рассматриваться как одна из приоритетных задач в обеспечении национальной безопасности страны.

Настоящее учебное пособие представляет собой попытку системного изложения проблем защиты информации, а также теоретических основ применения добавочных средств защиты. В пособии рассматриваются подходы к построению встроенных средств защиты современных операционных систем и приложений, выявлению причин их уязвимости на основе существующей статистики угроз. На основании этого формулируются и теоретически обосновываются общие требования к механизмам защиты, в том числе излагаются подходы к построению добавочных средств.

Целью учебного пособия является не только рассмотрение перспективных технологий и методов защиты информации от несанкционированного доступа (НСД), но и обоснование требований к системе защиты. Эти требования позволят ориентироваться на рынке средств защиты информации при выборе оптимального решения. Кроме того, в пособии немалое внимание уделено иллюстрации тех задач, которые должны решаться администратором безопасности, эксплуатирующим средства защиты. При этом следует понимать, что хорошая система защиты -- это своего рода "конструктор", в котором заложены механизмы противодействия как явным, так и скрытым угрозам информационной безопасности. Чтобы достигнуть необходимого уровня безопасности защищаемых объектов, специалист по защите информации должен не только знать и понимать возможности механизмов защиты, но и умело их настраивать применительно к непрерывно изменяющейся статистике угроз.

Об авторах

БОРИСОВ Михаил Анатольевич

Доцент факультета военного обучения при Московском государственном университете имени М. В. Ломоносова. Квалифицированный специалист в области защиты информации. Имеет многолетний практический опыт работы в структурных

подразделениях по защите государственной тайны различных уровней. На протяжении последних нескольких лет является ведущим преподавателем курса дисциплин специальности «Защита информационных технологий» на факультете военного обучения МГУ, а также дисциплин «Правовая и организационная защита информации», «Основы менеджмента защиты информации» и «Экономика защиты информации» в ряде образовательных учреждений. Автор более 30 учебно-методических изданий и научных публикаций.

ЗАВОДЦЕВ Илья Валентинович

Кандидат технических наук, доцент. Квалифицированный специалист в области комплексной защиты информации на объектах информатизации. Имеет многолетний практический опыт работы в структурных подразделениях по защите государственной тайны различных уровней. На протяжении последних нескольких лет является ведущим преподавателем учебных дисциплин «Программно-аппаратная защита информации», «Защита информационных процессов в компьютерных системах», «Организационная защита информации», «Обеспечение безопасного электронного документооборота» в Кубанском государственном технологическом университете и в филиале Военной академии связи в г. Краснодаре. Автор более 70 научных трудов и научно-популярных статей.

ЧИЖОВ Иван Владимирович

Кандидат физико-математических наук. Квалифицированный специалист в области построения систем комплексной защиты информации как в интересах органов государственной власти, так и для различных бизнес-структур. На протяжении последних нескольких лет читает курс лекций по программно-аппаратным средствам и методам защиты информации для магистров факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова, обучающихся по направлению «Прикладная математика и информатика». Автор 9 научных публикаций. Участник многих научно-практических конференций и семинаров в области информационной безопасности.