КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМ ИНФОРМАЦИОННО-КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ БИБЛИОТЕК

В.М.Зима, компания “Эврика”
Санкт-Петербург, 196084, Московский пр. 118
v_zima@eureca.ru

Несмотря на совершенствование технологий в области информационно-компьютерной безопасности уязвимость компьютерных систем продолжает возрастать. Причины сложившегося состояния, с одной стороны, связаны с общими предпосылками, современными тенденциями в развитии компьютерных технологий и недостатками используемых компьютерных систем, а с другой – отсутствием системного подхода к разрешению проблемы информационно-компьютерной безопасности. Последний фактор приводит к ошибкам построения системы защиты и недостаткам в поддержании ее актуального состояния.

Анализ указанных причин, а также общесистемных требований, вытекающих из теории и практики защиты информации, позволил выработать базовые требования к системе информационно-компьютерной безопасности, соблюдение которых обеспечивает достижение необходимой степени защиты информации:

- ⇒ комплексное использование наиболее эффективных мер, средств и методов защиты;
- ⇒ соответствие законодательным актам и нормативным документам;
- ⇒ наличие и полнота реализации всех приоритетных функций защиты;
- ⇒ способность к поэтапному внедрению без нарушения полной работоспособности защищаемой системы;
- ⇒ интеграция с полноценной службой каталогов для централизованного управления пользователями и ресурсами компьютерной сети;
- ⇒ способность к адаптации при изменении структуры, технологических схем или условий функционирования компьютерной сети;
- ⇒ поддержка возможности обновления общесистемного ПО с целью устранения имеющихся ошибок;
- ⇒ простота и удобство установки, эксплуатации, администрирования и сопровождения.

К сожалению, в настоящий момент на рынке технических систем информационной безопасности нет продуктов, полностью соответствующих всем перечисленным условиям. Высокие функциональные, эксплуатационные и нормативные требования не позволяют в рамках одного продукта реализовать все необходимые возможности. Кроме того, следует понимать, что даже наличие совершенных технических средств защиты не является достаточным условием построения эффективной системы информационно-компьютерной безопасности. Любой недостаток компьютерной системы, любая ошибка, допущенная при разработке или использовании программно-аппаратных средств, администрировании системы защиты является потенциальной угрозой. Именно по этой причине проблема информационно-компьютерной безопасности не может быть решена в рамках фрагментарного подхода, ориентированного на противодействие строго определенным угрозам при определенных условиях. Кроме того, эту проблему невозможно решить в общем случае, так как конкретные компьютерные системы отличаются друг от друга и эксплуатируются в разных условиях разными людьми. Выходом является лишь комплексный, системный подход к решению проблемы информационно-компьютерной безопасности.

В соответствии с комплексным подходом защита информации заключается не просто в создании соответствующих подсистем, а представляет собой регулярный процесс, осуществляемый на всех этапах жиз-

ненного цикла компьютерной системы при комплексном использовании наиболее эффективных мер, средств и методов защиты. Совокупность разработанных мер, средств и методов защиты должна быть достаточной для поддержания требуемой степени информационно-компьютерной безопасности в условиях появления новых угроз электронной информации. Особенность комплексного подхода состоит в создании защищенной среды автоматизированной обработки и хранения электронной информации, объединяющей все возможные меры защиты – технические, организационные, законодательные, морально-этические.

Система информационно-компьютерной безопасности должна обеспечить защиту от нанесения любого материального, морального или иного ущерба, который может произойти по причине случайных или преднамеренных воздействий на информацию и процесс ее обработки. Соответственно необходимо поддержание конфиденциальности, целостности, подлинности и доступности информации. Достижение перечисленных целей требует качественного решения следующих задач:

1) защиты подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;
2) защиты информации в процессе передачи по открытым коммуникациям;
3) защиты компьютерных ресурсов на уровне серверов, а также локальных и удаленных рабочих станций;
4) поддержания подсистем информационно-компьютерной безопасности в актуальном состоянии.

Выступая в роли системного интегратора, с учетом выработанных требований и базовых принципов защиты информации, возможно промышленное производство защищенных гетерогенных автоматизированных систем, основанных на сертифицированных в России средствах защиты информации, к которым относятся:

⇒ комплексы многоуровневой защиты компьютерных ресурсов “АккордСеть-NDS”, Secret Disk, Secret Net, СПЕКТР-Z и др.;

⇒ средства криптографической защиты информации семейства “Верба”;

⇒ межсетевые экраны (FireWall-1, Aker, BorderManager и др.), а также основанные на них средства построения защищенных виртуальных сетей;

⇒ средства контроля защищенности (Nessus, Internet Scanner, System Scanner, Database Scanner и др.);

⇒ средства обнаружения атак в режиме реального времени (RealSecure, BlackICE и др.);

⇒ средства защиты, входящие в состав Novell Netware 5, NDS, Windows NT/2000, UNIX.

Результаты апробации многих технических решений позволяют сделать вывод, что защищенные автоматизированные системы, построенные на основе комплексного подхода и различных классов сертифицированных в России средств защиты, могут реально соответствовать отечественным и международным стандартам в области информационно-компьютерной безопасности и обеспечивают надежную защиту компьютерных ресурсов и конфиденциальной информации.

THE COMPREHENSIVE APPROACH TO CONSTRUCTION THE COMPUTER SECURITY SYSTEMS OF ELECTRONIC LIBRARIES

V.M.Zima, EURECA company
St.-Petersburg, 196084, Moscowsky pr., 118
v_zima@eureca.ru

Despite of perfecting of technologies in the field of information security the vulnerability of computer systems continues to increase. In the report the analysis of reasons of the current state will be carried out and the comprehensive approach to solution of a problem of computer security is considered. The feature of the offered comprehensive approach consists in creation of the protected environment of the atomised processing and storage of the electronic information joining all possible measures of protection - technical, organisational, legislative, ethical. The examples of complex technical solutions appropriate to domestic and international standards in the field of computer security and providing reliable protection of computer resources and the confidential information are resulted.