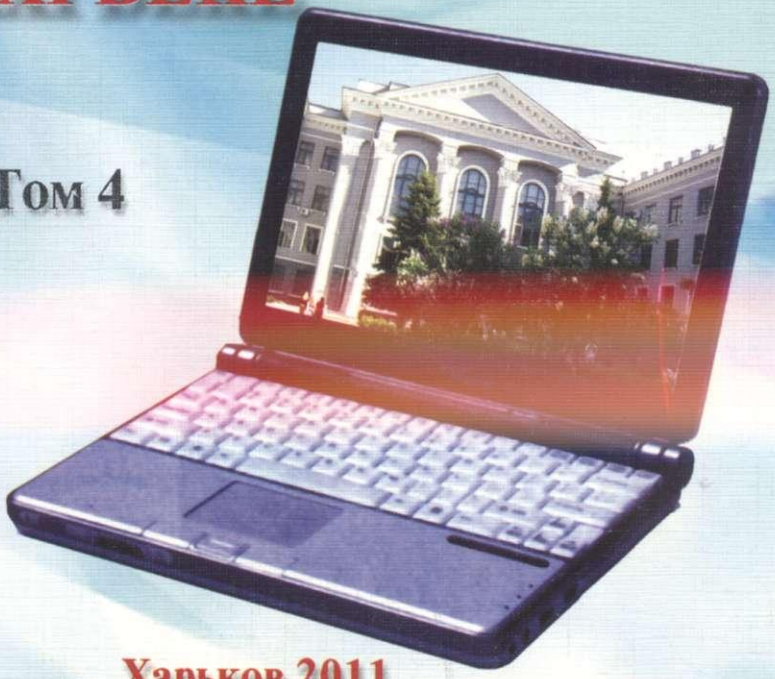
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ,
МОЛОДЕЖИ И СПОРТА УКРАИНЫ
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

МАТЕРИАЛЫ XV МЕЖДУНАРОДНОГО МОЛОДЕЖНОГО ФОРУМА

РАДИОЭЛЕКТРОНИКА И МОЛОДЕЖЬ В XXI ВЕКЕ



Том 4

Харьков 2011

АНАЛИЗ НЕОБХОДИМОГО УРОВНЯ ДЕТАЛИЗАЦИИ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Николаенко О.А.
Научный руководитель — к.т.н., ст. прп. Токарь Л.А.
Харьковский национальный университет радиоэлектроники
(Адрес: 61166, Харьков, пр.Ленина 14, т. (057) 702-13-20
e-mail: jobleka@gmail.com)

The effectiveness of the security facilities of information systems is the most important characteristic that requires the development of conceptual proposals on the basis of detailed threats defined object type.

Система обеспечения безопасности имеет сложную структуру и включает правовые, организационные, технологические, технические, информационные и другие составляющие, что осуществляется в рамках многофункциональных организационно-технических систем технической защиты информации (ТЗИ), формируемых на государственном уровне, а также на уровне отдельных предприятий и организаций.

Существующие подходы и системы требований к обеспечению безопасности требуют корректировки как на нормативном, так и на техническом уровне, особенно на критически важных объектах (экологически опасных, ядерных, военных объектах, включая объекты жилищной и социальной сферы, коммуникаций и транспортной инфраструктуры).

Научно-методический аппарат, существующий в настоящее время, разработан с целью повышения безопасности на особо важных объектах, и включает следующие основные направления: анализ уязвимости объектов, оценку эффективности систем безопасности.

Активное внедрение информационных технологий в деятельность предприятий и организаций влечет за собой повышение уровня угроз информационной безопасности, а именно: угроз информационным системам, утечки и преднамеренный сбор информации.

Информационные системы предприятий и объектов снабжаются подсистемой информационной безопасности, для построения которой необходимы следующие условия: стыковка и обмен информацией с информационными системами, средства системы информационной безопасности и находящаяся в них информация сами по себе нуждаются в защите собственным сегментом.

Объем и характер защитных мер, предпринимаемых в отношении объектов информационных систем, определяется с учетом величины и значимости потенциальных потерь, т.е. с необходимой степенью детализации.

Система обеспечения безопасности объединяет совокупность баз данных пользователей, каждая из которых может быть представлена смысловой и логической структурой, которые представляют собой необходимые уровни детализации.

На уровне смысловой структуры баз данных сравниваются группы данных, включаемые в минимально необходимый для решения задач пользователей набор групп данных. На уровне логической структуры сравниваются совокупности логических записей и связей между ними, отражающие смысловое содержание, функциональные свойства и особенности информационных систем и используются при решении функциональных задач. В результате способ организации и хранения данных для существующей информационной системы представляется вариантом смысловой и логической структуры включаемых в эту систему баз данных.

Целесообразность степени обеспечения безопасности объектов информационных систем состоит в выборе минимально необходимого перечня угроз, определяемого типом объекта, что обеспечит выполнение требований к качеству решения функциональных задач на базе имеющихся средств, а также соответствие системы реальным требованиям по безопасности объекта.

При расширении функций информационных систем возникает необходимость расширения состава, функций, задач, совершенствования видов обеспечения безопасности, что предполагает совершенствование характеристик подсистем безопасности, параметров их элементов, программного обеспечения и многих других компонентов.

Список использованных источников

- Методические основы структурирования информации интересах автоматизации решения задач в области технической защиты информации/ Головин С.А. и др.Информация и безопасность, 2003, №2, с.40-46.
- Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0,1,2-96.
- Угрозы безопасности/ Мусиенко Д..Бизнес и безопасность, 2008, №2, с.43-56.