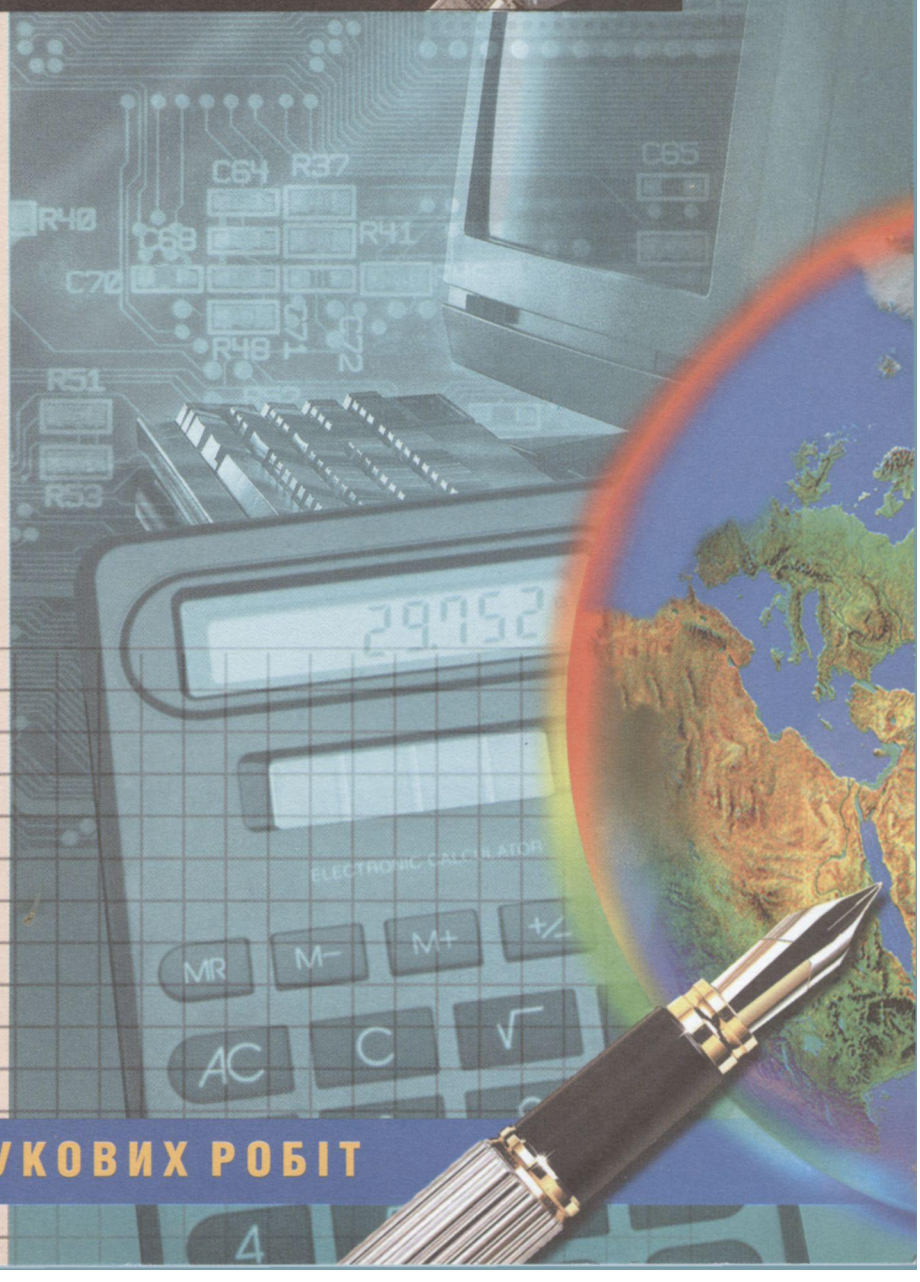
Управління розвитком

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ



№ 7, 2008

ЗБІРНИК НАУКОВИХ РОБІТ

Управління розвитком

Харківський національний економічний університет

І міжнародна науково-практична конференція "Безпека та захист інформації в інформаційних і телекомунікаційних системах"

Секція 1
"Методи та технології безпеки інформаційних систем"

Секція 2
"Захист інформації в комп'ютерних системах"

Секція 3
"Інформаційні та телекомунікаційні системи в бізнесі"

28 – 29 травня 2008 року

Збірник наукових статей

видається 2 рази на рік

№ 7, 2008

Харків. Вид. ХНЕУ, 2008

ЗБІРНИК НАУКОВИХ СТАТЕЙ

Управління РОЗВИТКОМ

№ 7' 2008

Засновник і видавець

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Реєстраційний номер свідоцтва КВ №5948 від 19 березня 2002 р.

Затверджено на засіданні вченої ради університету.

Протокол №9 від 21.04.2008 р.

Адреса видавця: *61001, Україна, м. Харків, пр. Леніна, 9а*

Телефони:
(057)702-03-04 – головний редактор
(057)758-77-05 – зав. редакції

E-mail: *vydav@ksue.edu.ua*

Підписано до друку 19.05.2008 р.
Формат 84×108 1/16. Папір MultiCopy.
Ум.-друк. арк. 12,0. Обл.-вид. арк. 15,12. Тираж 500 прим. Зам. № 409.
Ціна договірна.

Надруковано з оригінал-макета на Riso-6300 61001, м. Харків, пр. Леніна, 9а.
Видавництво ХНЕУ.

Менее исследованными являются ТКУИ, образованные применением различных типов аппаратных закладок (АЗ). Основные проблемные аспекты здесь обусловлены априорной неопределенностью о видах и характеристиках применяемых АЗ. Ситуация усугубляется необходимостью аттестации не только средств ЭВТ, обрабатывающих информацию с ограниченным доступом, но и помещений, где они установлены [4; 5].

В качестве примера рассмотрены существующие методы активной (на базе сетевых генераторов шума) [6] и пассивной (на основе сетевых помехоподавляющих фильтров) [7] защиты электрических ТКУИ, образованных мощными узкополосными (кварцованными) сетевыми АЗ в целях аудиоконтроля выделенных помещений.

Показано теоретически и проверено экспериментально, что на выходе отечественных сертифицированных помехоподавляющих фильтров серии "М" (ЗАО "Сетевые технологии", г. Нетишин) и ФМПЗ (НТУУ "КПИ", г. Киев) в условиях априори неизвестной рабочей частоты сетевой АЗ [8] могут присутствовать остатки неподавленных информативных сигналов, величина которых на 7–10 дБ превышает пороговую чувствительность существующих разведприемников, что и обуславливает возможность утечки информации по такому каналу.

Таким образом, в данных условиях целесообразно сочетание активных и пассивных методов блокирования [9], предложено и исследовано реализующее устройство защиты.

Литература: 1. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб.: Питер, 2008. – 320 с. 2. Хорев А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи // Специальная техника. – 1998. – №2. – С. 41 – 46. 3. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 504 с. 4. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М.: Горячая линия-Телеком, 2005. – 416 с. 5. Временные рекомендации по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам побочных электромагнитных излучений и наводок (ВР ЭВТ–95)// Безопасность информации. – 1995. – №2. – С. 54 – 57. 6. Емельянов С. Проблемные аспекты реализации пространственного и линейного зашумления в системах активной защиты информации / С. Емельянов, Н. Логвиненко, В. Носов, В. Писаревский // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – №2. – С. 135 – 138. 7. Емельянов С. Л. Эффективность фильтрации информативных сигналов в электрических каналах утечки информации // Труды восьмой международной научно-практической конференции "Современные информационные и электронные технологии". Одесса, 21 – 25 мая 2007 г. – Одеса. СИЭТ, 2007. – С. 179. 8. Емельянов С. Л. К вопросу выбора рабочего диапазона частот сетевых закладных устройств аудиоконтроля / С. Емельянов, В. Гаращук //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – №1(12). – С. 158 – 162. 9. Методы борьбы с сетевыми закладными устройствами // Матеріали третьої міжн. наук.-практ. конф. "Наукові дослідження – теорія та експеримент 2007" Т.7. Полтава,14 – 16 травня 2007 р. – Полтава: "ІнтерГрафіка", 2007. – С. 135.

УДК 007:330

Охрименко С. А.

Тутунару С. А.

Склифос К. Ф.

ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время информационное пространство современного общества объединяет информационные ресурсы, информационные технологии и информационную инфраструктуру предприятий и организаций, коллективных и индивидуальных пользователей. Наше общество постоянно сталкивается не только с проблемами экономического, социального и экологического характера, но и информационного. В среде комплекса информационных проблем ведущее место принадлежит информационной безопасности.

Проблема информационной безопасности носит комплексный характер и объединяет сочетание правовых, организационных и программно-технических мер. В последнее время отмечается пристальный интерес к экономическим аспектам информационной безопасности. Этот интерес

объясняется не только увеличением затрат на обеспечение информационной безопасности, которые отмечаются повсеместно, но и необходимостью представления экономических выкладок для разъяснения важности и целесообразности вложений в информационную безопасность для существующего бизнеса.

Экономика информационной безопасности (ЭИБ), как самостоятельное научное направление, получило развитие в 90-х годах прошлого столетия [1–6]. Истоками данного направления следует считать комплекс исследований и практических разработок, связанных с такими факторами, как:

процессы совершенствования организационных форм использования вычислительной техники;

замена вычислительной базы и переход к использованию новых информационных и коммуникационных технологий;

разработка операционных систем для персональных компьютеров;

появление специфических угроз (компьютерных вирусов);

реализация атак на информационные системы и др.

«Идеальная» система информационной безопасности должна объединять в себе комплекс мер, таких, как правовые, организационные, технические, экономические и морально-этические. Но создание именно «идеальной» системы возможно только по отношению к государственным информационным системам, чьи ресурсы защищаются специальными подразделениями. Применительно к деятельности коммерческих структур процессы проектирования, внедрения и эксплуатации СИБ сопряжены с огромными затратами, требуют наличия высококвалифицированных кадров и т. д., что является не всегда доступным.

В работе рассмотрены основные проблемы формирования ЭИБ как новой учебной дисциплины. Данная дисциплина, по мнению авторов, является на сегодняшний момент наиболее актуальной, поскольку специалисты уделяют все большее внимания вопросам экономической эффективности систем информационной безопасности. Отмечается общая тенденция роста стоимости работ по информационной безопасности, так как процессы проектирования, внедрения и эксплуатации системы информационной безопасности сопряжены с огромными затратами на программные и технические средства, требуют наличия высококвалифицированных кадров и т. д.

В рамках данного направления выделяются работы, связанные с исследованием комплекса показателей экономической эффективности, разработкой экономико-математических моделей, управлением риском и др. [7–9]. Необходимо детальное изучение методов расчета эффективности системы информационной безопасности, поскольку именно они характеризуют инвестиционную привлекательность. К их числу относят следующие:

суммарная стоимость владения TCO (Total Cost of Ownership);

чистая приведенная стоимость NPV (Net Present Value);

внутренняя норма рентабельности IRR (Internal Rate of Return);

экономическая привлекательность EVA (Economic Value Added);

сбалансированная балльная оценка BSC (Balanced Score-card).

Особое внимание, по мнению авторов, должно уделяться подготовке и разработке организационно-распорядительной документации, которая интегрирует теоретические знания и практические навыки, полученные в процессе освоения основных разделов данного предмета.

Представленный материал отражает только точку зрения авторов и не может претендовать на завершенность. Вполне очевидно, что данный предмет может быть дополнен новыми разделами, отражающими современные теоретические знания и практические навыки, используемыми для разрешения кризисных ситуаций в управлении системами информационной безопасности, а также соответствовать требованиям международных и национальных стандартов.

Литература: 1. Галицын В. К. Планирование на предприятиях информационно-вычислительного обслуживания / В. К. Галицын, С. П. Куценко, М. И. Кутер, С. Ф. Лазарева. – К.: Техника, 1991. – 221 с. 2. Герасименко В. А. Основы защиты информации в автоматизированных системах обработки данных. – М.: ВИНИТИ, N 1080-В-91, 1991. – 478 с. 3. Доветов М. Ш. Экономика и организация вычислительных установок / М. Ш. Доветов, В. А. Залесов. – М.: Финансы и статистика, 1982. – 303 с. 4. Новицкас Ю. М. Экономика ЭВМ. – Ленинград: Машиностроение, 1983. – 176 с. 5. Экономика индустрии информатики / Под ред. Ю. М. Каныгина, А. М. Меняйло. – Красноярск: Изд-во Краснояр. Ун-та, 1987. – 336 с. 6. Якушенко В. Г. Планирование, учет и анализ деятельности хозрасчетных вычислительных установок. – М.: Статистика, 1980. – 112 с. 7. Rachel Rue. A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. Rachel Rue, Shari Lawrence Pfleeger and David Ortiz // Workshop on the Economics of Information Security (2007). 8. Gritzalis S. A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments / S. Gritzalis, A. N. Yannacopoulos, C. Lambrinoudakis, P. Hatzopoulos, S. K. Katsikas // Int. J. Inf. Secur. (2007) 6:197–211. 9. Sklavos Nicolas. Economic Models and Approaches in Information Security for Computer Networks / Nicolas Sklavos, Panagiotis Souras International Journal of Network Security. – Jan. 2006. – Vol.2. – №1. – P.14 – 20.

Зміст

Секція 1
Методи та технології безпеки інформаційних систем

Секція 2
Захист інформації в комп'ютерних системах