мика: проблемы теории и практики". Днепропетровск: Изд. Руснаука, 2009. – т. 246. – № 4. – С. 862-869.
5. Олейников Е. А. Экономическая и национальная безопасность: Учебникдля вузов. – М.: Экзамен, 2005. – 768 с.
6. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк.– Х.: ХНЕУ, 2006. – 240 с.
7. Гуров М.П., Кудрявцев Ю.А. Теневая экономика и экономическая преступность в вопросах и ответах: Учебное пособие. - СПб.: Санкт-Петербургский университет МВД России, 2002. - 237 с.

ФОРМИРОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОРГОВОЙ КОМПАНИИ

С. В. КАРПЕНКО, Е.В. ПРОКОФЬЕВА
Белорусский торгово-экономический университет потребительской кооперации (Гомель, Республика Беларусь)

В сфере информационных технологий растет объем предложений по обеспечению безопасности информационных систем. Действия служб, направленные на повышение уровня информационной безопасности, не приносят доходов, но с их помощью можно уменьшить потери от возможных инцидентов.

Потребности организации в некотором уровне защищенности автоматизированной системы можно определить, воспользовавшись руководящими стандартами СТБ 34.101.1 - 2001(ИСО/МЭК 15408-1-99), ("Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий").

Требования к автоматизированным системам защиты обобщены в таблице 1, где выполнен анализ системы защиты информации, условно состоящей из следующих четырех подсистем: подсистема управления доступом; подсистема регистрации и учета; криптографическая подсистема; подсистема обеспечения целостности.

Таблица 1

Требования к автоматизированным системам защиты

Подсистемы и требования	Класс 3	Класс 2	Класс 1

Анализ данных таблицы и сопоставление ее характеристик с реальными характеристиками технологий и программных продуктов предприятия позволяет говорить о принадлежности корпоративной информационной системы компании к 1 классу и отметить достаточно высокий уровень соответствия.

При этом отмечен ряд недостатков системы. Они определяют направления совершенствования системы защиты организации. Даны рекомендации для развития 4-х перечисленных подсистем.

Для совершенствования информационной системы «Алеси» на основе разделения доступа к информационных ресурсам выполнено категорирование информации**. Использованы два подхода:**

1. Категорирование безопасности информации и информационных систем на основе оценки ущерба
2. Категорирование безопасности информации и информационных систем с точки зрения критичности.

Представлены результаты, внедренные в практику работы Алеси.

Проведенное категорирование информации для информационной системы «Алеси» позволило выполнить разделение прав доступа к информационным ресурсам корпоративной системы.

Формирование прав доступа для пользователей и групп пользователей ОАО НТК «Алеся» находится в состоянии разработки. Рассмотрены направления их совершенствования, а также вопросы администрирования программного комплекса «SBC - предприятие» в данном аспекте.

Распределение доступа к основным группам электронных документов. В ОАО НТК «Алеся» авторизованными субъектами являются все работники предприятия, которые имеют в своем распоряжении ПК. Механизмы управления доступом субъектов к объектам информации выполняют основную роль в обеспечении внутренней безопасности компьютерных систем. Их работа строится на концепции единого диспетчера доступа. Сущность этой концепции состоит в том, что диспетчер доступа (монитор ссылок) - выступает посредником-контролером при всех обращениях субъектов к объектам. Схема работы механизма разграничения доступа к информационным ресурсам включает: правила разграничения доступа, диспетчер доступа, субъекты доступа (работники предприятия), объекты доступа (папки с документами, электронные документы).

Диспетчер доступа обязан выполнять следующие основные функции:

- проверяет права доступа каждого субъекта к конкретному объекту на основании информации, содержащейся в базе данных разграничения доступа хранящейся на главном офисном сервере ОАО НТК «Алеся»;
- разрешает (производит авторизацию) или запрещает (блокирует) доступ субъекта к каталогу, документу;
- при необходимости регистрирует факт доступа и его параметры в системном журнале (в том числе попытки несанкционированного доступа с превышением полномочий).

Основными требованиями к реализации диспетчера доступа являются:

- полнота контролируемых операций (проверке должны подвергаться все операции всех субъектов над всеми объектами системы, - обход диспетчера предполагается невозможным);

- изолированность диспетчера, то есть защищенность самого диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;

Форма представления базы данных защиты может быть различной.

Основу базы данных средств разграничения доступа в общем случае составляет абстрактная матрица доступа или ее реальные представления. Каждая строка этой матрицы соответствует субъекту, а столбец - объекту АИС.

Разработана матрица распределения доступа к основным группам электронных документов для сотрудников ОАО НТК «Алеся», представленная в виде таблицы. По вертикали 13 субъектов, по горизонтали 9 объектов. На пересечении – варианты доступа: полный доступ, чтение, нет доступа, создание.

Представлены права для следующих категорий пользователей: 1) администратор баз данных или администратор системы (инженер программист), 2) пользователи 1-го уровня доступа (бухгалтер, экономист, сотрудники коммерческого отдела; товароведы; работник строительной группы; сотрудник инженерной службы финансист; специалисты отдела кадров; ревизионной службы и т.д.), 3) пользователи 2-го уровня доступа (начальники всех отделов; кассиры торговой сети; заведующие магазинами; генеральный директор; операторы терминалов).

Предложены возможные сценарии работы по разграничению прав доступа группам пользователей к информационным ресурсам АИС «SBC - предприятие».

Администратор баз данных может создавать, копировать, читать, и удалять электронные документы. Факт удаления электронного документа должен быть отражен в регистрационном журнале.

Систему санкционирования доступа целесообразно строить на основе структурно-функционального (задачного) подхода к разделению всего множества защищаемых ресурсов АИС. Отдельная задача должна описывать все используемые при ее решении ресурсы (файлы, каталоги, таблицы БД и т.п.), все категории пользователей (роли в задаче) и права доступа для каждой такой категории к ресурсам задачи. Описания задач в виде формуляров должны формироваться с участием специалистов по сопровождению данных задач и системных администраторов (администраторов баз данных) и могут храниться в архиве эталонных дистрибутивов программ.

Полномочия руководителей отделов давать разрешения на допуск к решению тех или иных задач должны быть закреплены решениями (приказами) высшего руководства организации. Как правило, задачи закрепляются за конкретными подразделениями, а права допуска сотрудников этих подразделений к ресурсам этих задач предоставляются руководителям подразделений.

Важно, чтобы затраты на создание и поддержание безопасности информационных систем и её уровень были соизмеримы.