рисками информационной безопасности BS 7799-3:2006. – С. 70. ***2.*** *Koshko, B Fuzzy Congnitive Maps / B. Koshko // Int. J. of Man-Machine Studies. – 1986. – Vol. 1. – P.65 – 75.* ***3.*** *Хрусталёв Е. Когнитивные технологии в теории и практике стратегического управления (на примере оборонно – промышленного комплекса), 2007. – С. 25–33.*

УДК 681.3.06

ЗАЩИТА ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ОПЕРАЦИОННЫХ СИСТЕМ MS WINDOWS

Андрей Тимошенко
ООО "Институт компьютерных технологий"

Анотація: **Розглянуто проблеми забезпечення захисту інформації з обмеженим доступом в інформаційних системах на базі локальних обчислювальних мереж, побудованих із використанням комп'ютерів під керуванням операційних систем сімейства MS Windows.**
Summary: **The problems of critical information security in computer systems, based on the local area networks and computers with MS Windows operating systems are discussed.**
Ключові слова: **Інформаційна система, захист інформації.**

В настоящее время трудно представить себе предприятие или организацию, в которой не используются автоматизированные (информационные) системы, реализующие различные технологии обработки информации. В качестве основы вычислительной системы таких информационных систем (ИС), как правило, выступают локальные вычислительные сети (ЛВС) – совокупность взаимодействующих в процессе своего функционирования компьютеров, имеющих совместно используемые (разделяемые) ресурсы (жесткие диски, устройства печати и т. п.). Современные ЛВС обычно подразделяют на одноранговые – такие, в которых совместно использоваться (разделяться) могут ресурсы любого компьютера, который, таким образом, может выполнять роль как клиентской рабочей станции, так и роль невыделенного сервера, а также ЛВС с выделенными серверами – такие, в которых совместно используются ресурсы только специально выделенных компьютеров (серверов). При этом подавляющее большинство современных ЛВС, как одноранговых, так и с выделенными серверами, строятся с использованием компьютеров (рабочих станций, невыделенных и выделенных серверов), функционирующих под управлением операционных систем (ОС) семейства MS Windows. На сегодняшний день в качестве ОС рабочих станций, как правило используется MS Windows XP или MS Windows 7, а в качестве ОС серверов – MS Windows Server 2003 или MS Windows Server 2008.

Согласно НД ТЗИ 2.5-004-99 [1], ИС, о которых идет речь, могут быть классифицированы: как автоматизированные системы (АС) класса 2 – в случае, если вычислительная система ИС имеет территориально локализованный характер и построена на основе одной ЛВС; как АС класса 3 – в случае, если вычислительная система ИС имеет территориально распределенный характер и построена на основе нескольких территориально локализованных ЛВС, взаимодействие между которыми организовано с использованием каналов распределенных сетей передачи данных, например, ведомственных сетей или сети Интернет.

Целью данной статьи является анализ особенностей обеспечения защиты информации с ограниченным доступом (ИсОД), обрабатываемой в ИС, классифицируемых как АС класса 2, либо в отдельных составляющих ИС, классифицируемых как АС класса 3, при условии, что в качестве основы вычислительной системы этих ИС выступают ЛВС, построенные с использованием компьютеров, функционирующих под управлением ОС семейства MS Windows (далее – ИС на базе ЛВС). Вопросы, касающиеся защиты данных, передаваемых по каналам распределенных сетей передачи данных, не рассматриваются.

Любая информационная (автоматизированная) система [2] представляет собой организационно-техническую систему, объединяющую вычислительную систему, физическую среду, в которой функционируют компоненты вычислительной системы ИС, персонал и обрабатываемую информацию. При этом, кроме характеристик обрабатываемой информации и физической среды, одной из ключевых характеристик ИС, непосредственно влияющих на функциональный и структурный состав реализуемого комплекса средств защиты (КСЗ) информации, является архитектура вычислительной системы ИС, в

первую очередь, архитектура прикладных программных средств (ППС), непосредственно реализующих соответствующую технологию обработки информации (информационную технологию).

Архитектура ППС современных ИС на базе ЛВС, как правило, относится к одному из следующих типов: файл-серверная, двухуровневая клиент-серверная, трехуровневая клиент-серверная.

Файл-серверная архитектура – архитектура ППС, предполагающая централизованное хранение обрабатываемой в ИС информации на выделенных или невыделенных серверах ИС и ее децентрализованный ввод и обработку на рабочих станциях ИС. Основной особенностью файл-серверной архитектуры ИС с точки зрения реализуемой технологии обработки информации является то, что вся обрабатываемая информация централизованно сохраняется (в виде структурированных или неструктурированных файлов данных) с использованием штатных средств соответствующей ОС на разделяемых ресурсах запоминающих устройств (жестких дисков) серверов ИС, при этом все операции по ее вводу/ модификации/ обработке выполняются в клиентских приложениях, функционирующих на рабочих станциях ИС. В процессе обработки информации на рабочих станциях ИС она может (при необходимости) сохраняться в виде отдельных файлов данных на неразделяемых ресурсах запоминающих устройств (жестких дисков) соответствующих рабочих станций, импортироваться в систему с использованием съемных носителей или различных устройств ввода информации, экспортироваться из системы с использованием съемных носителей, выводиться на устройства печати и/или другие внешние устройства. Примером использования файл-серверной архитектуры может служить ИС, в которой создаваемые файлы документов сохраняются на разделяемых жестких дисках серверов ИС, а обрабатываются в программных средствах пакета MS Office, функционирующих на рабочих станциях ИС.

Двухуровневая клиент-серверная архитектура – архитектура ППС, предполагающая централизованное хранение и обработку информации на выделенных или невыделенных серверах ИС и децентрализованный доступ к информации и результатам ее обработки на рабочих станциях ИС. Основной особенностью двухуровневой клиент-серверной архитектуры с точки зрения реализуемой технологии обработки информации является то, что вся обрабатываемая информация централизованно сохраняется (как правило, в виде структурированных файлов данных) на разделяемых ресурсах запоминающих устройств (жестких дисков) серверов ИС с использованием не только штатных средств ОС, а и специализированных программных средств (серверов системы управления базой данных (СУБД), выполняющих также функции серверов приложений), функционирующих на серверах ИС, а также централизованно обрабатывается в программных средствах серверов приложений (серверов СУБД), функционирующих на серверах ИС. При этом операции по вводу/модификации информации выполняются в специализированных клиентских приложениях, функционирующих на рабочих станциях ИС и взаимодействующих с соответствующими серверами приложений. В процессе обработки информации на рабочих станциях ИС она может (при необходимости) сохраняться в виде отдельных файлов данных на неразделяемых ресурсах запоминающих устройств (жестких дисков) соответствующих рабочих станций, импортироваться в систему с использованием съемных носителей или различных устройств ввода информации, экспортироваться из системы с использованием съемных носителей, выводиться на устройства печати и/или другие внешние устройства. Примером использования двухуровневой клиент-серверной архитектуры может служить ИС, в которой специализированный сервер приложений построен на базе сервера промышленной СУБД, например, Oracle или MS SQL Server, а в качестве клиентских приложений используются так называемые "толстые клиенты", реализующие необходимые прикладные функции.

Трехуровневая клиент-серверная архитектура – архитектура ППС, предполагающая централизованное хранение и обработку информации на выделенных или невыделенных серверах ИС и децентрализованный доступ к информации и результатам ее обработки на рабочих станциях ИС, но с разделением функций управления централизованным хранением и обработкой информации между различными серверами приложений (в качестве того, который используется для управление централизованным хранением информации, используется обычно сервер промышленной СУБД). Основной особенностью трехуровневой клиент-серверной архитектуры с точки зрения реализуемой технологии обработки информации является то, что вся обрабатываемая информация централизованно сохраняется (как правило, в виде структурированных файлов данных) на разделяемых ресурсах запоминающих устройств (жестких дисков) серверов ИС с использованием штатных средств ОС и специализированных программных средств (серверов СУБД), функционирующих на серверах ИС, а также централизованно обрабатывается в специализированных серверах приложений, функционирующих на тех же самых или других серверах ИС. При этом операции по вводу/модификации информации выполняются в специализированных клиентских приложениях, функционирующих на рабочих станциях ИС и взаимодействующих с соответствующими серверами приложений, которые, в свою очередь, взаимодействуют с серверами СУБД. В процессе обработки информации на рабочих станциях ИС она может (при необходимости) сохраняться в виде

отдельных файлов данных на неразделяемых ресурсах запоминающих устройств (жестких дисков) соответствующих рабочих станций, импортироваться в систему с использованием съемных носителей или различных устройств ввода информации, экспортироваться из системы с использованием съемных носителей, выводиться на устройства печати и/или другие внешние устройства. Примером использования трехуровневой клиент-серверной архитектуры может служить ИС, в которой в качестве сервера СУБД, используется MS SQL Server, специализированный сервер приложений реализован на базе MS Internet Information Services, а в качестве клиентских приложений используются так называемые "тонкие клиенты", реализованные на базе Internet Explorer.

Согласно положеням законодательства Украины [3 – 5], ИсОД, в том числе обрабатываемая в ИС на базе ЛВС, подразделяется на конфиденциальную, служебную и секретную. Порядок доступа к ИсОД, перечень пользователей и их полномочия касательно этой информации определяются владельцем информации, а в случаях, когда речь идет об ИсОД, являющейся собственностью государства, или ИсОД, требования к защите которой определяются законом – соответствующим законодательством. При этом требования к обеспечению защиты ИсОД, являющейся собственностью государства, или ИсОД, требования к защите которой определяются законом, устанавливаются Кабинетом Министров Украины. Проанализируем требования к обеспечению защиты ИсОД, установленные Кабинетом Министров Украины в соответствующих "Правилах обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах" [6] (далее – "Правила"), с учетом положений НД ТЗИ 2.5-008-2002 [7], который не только детализирует требования по защите ИсОД от несанкционированного доступа во время обработки в АС класса 2, но и устанавливает, в соответствии с определенными НД ТЗИ 2.5-004-99 спецификациями минимально необходимые перечни функциональных услуг безопасности (ФУБ) и уровней их реализации в КСЗ (стандартные функциональные профили защищенности), предназначенных для защиты ИсОД в таких АС.

"Правила" формулируют следующие задачи защиты, реализация которых должна быть обеспечена автоматизированным способом:

- защита от несанкционированного и неконтролируемого ознакомления с ИсОД (далее – З.ОЗН.ПР);
- защита от несанкционированной и неконтролируемой модификации или уничтожения ИсОД (далее – З.МОД.ПР);
- защита от несанкционированного и неконтролируемого копирования и распространения ИсОД (далее – З.КОП.ПР);
- обеспечение возможности предоставления пользователю прав на выполнение одной или нескольких операций по обработке ИсОД или лишение его такого права (далее – З.АДМ.ПР);
- предоставление доступа к ИсОД только идентифицированным и аутентифицированным пользователям, блокирование доступа к такой информации неидентифицированных и неаутентифицированных пользователей (далее – З.АУТ.ПР);
- защита доступности ИсОД на усмотрение распорядителя информации (далее – З.ДОСТ.ПР);
- регистрация критичных с точки зрения защиты информации событий (результатов идентификации и аутентификации пользователей; результатов выполнения операций по обработке ИсОД; попыток несанкционированного доступа к информации; фактов предоставления пользователям прав доступа к ИсОД и лишения их таких прав; результатов проверки целостности средств защиты информации) (далее – З.РЕГ.ПР);
- возможность выполнения анализа зарегистрированной информации уполномоченным администратором (далее – З.АНРЕГ.ПР);
- контроль целостности прикладного программного обеспечения ИС, используемого для обработки ИсОД, а также предотвращение его несанкционированной модификации (далее – З.ЦЕЛПО.ПР);
- контроль целостности средств защиты информации с блокированием обработки информации в случае нарушения их целостности (далее – З.ЦЕЛКСЗ.ПР).

НД ТЗИ 2.5-008, с учетом корректировок его положений, которые следуют из принятых после его введения в действие "Правил", формулируют следующие задачи защиты, реализация которых автоматизированным способом является обязательной для защиты ИсОД:

- определение средствами КСЗ нескольких иерархических уровней полномочий пользователей и нескольких классификационных уровней информации (далее – З.УРП.НД);
- возможность предоставления пользователям санкционированного и контролируемого доступа к ИсОД только при наличии служебной необходимости (далее – З.АДМ.НД);
- запрет несанкционированной и неконтролируемой модификации ИсОД (далее – З.ЦЕЛ.НД);

- осуществление учета выходных данных, полученных во время решения функциональных задач в форме отпечатанных документов, которые содержат ИсОД (далее – З.УЧ.НД);
- запрет несанкционированного копирования, размножения, распространения ИсОД в электронном виде (далее – З.КОП.НД);
- обеспечение возможности своевременного доступа зарегистрированных пользователей к ИсОД (далее – З.ДОСТ.НД);
- осуществление однозначной идентификации и аутентификации каждого зарегистрированного пользователя (далее – З.АУТ.НД);
- обязательность регистрации в ИС всех пользователей и их действий по доступу к конфиденциальной информации (далее – З.РЕГ.НД);
- обеспечение контроля за санкционированным копированием, размножением, распространением ИсОД в электронном виде (далее – З.КОНТР.НД).

При этом основными информационными ресурсами, подлежащими защите в системах обработки ИсОД, являются:

- информационные объекты (ИО), содержащие ИсОД и требующую защиты открытую информацию, представляющие собой совокупность сильносвязанных объектов (под сильносвязанными объектами понимается совокупность наборов данных, которые характеризуются наличием минимальной избыточности и допускают их оптимальное использование одним или несколькими процессами как одновременно, так и в разные промежутки времени и требуют безусловного обеспечения целостности этих наборов данных как совокупности, например, совокупность связанных таблиц базы данных или иных информационных объектов в хранилищах специализированных серверов приложений);
- ИО, содержащие ИсОД и требующую защиты открытую информацию, представляющие собой слабосвязанные объекты различного вида представления (относительно независимые наборы данных, которые генерируются, модифицируются, сохраняются и обрабатываются в системе и требуют обеспечения своей целостности каждый в отдельности, в виде, например, отдельных файлов данных).

Для различных технологий обработки ИсОД сформулированы функциональные профили защищенности информации и требования к политике соответствующих ФУБ:

- в случае применения технологии, выдвигающей повышенные требования к обеспечению конфиденциальности и целостности обрабатываемой информации: *2.КЦ.3 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}*;
- в случае применения технологии, выдвигающей повышенные требования к обеспечению конфиденциальности, целостности и доступности обрабатываемой информации: *2.КЦД.2а = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}*.

При этом указывается, что, разграничение доступа должно осуществляться в соответствии с административным принципом управления доступом, а реализация ФУБ, которые базируются на доверительном принципе разграничения доступа, может осуществляться в случаях, когда политикой безопасности предусмотрено создание групп пользователей с одинаковыми полномочиями по работе с ИсОД для разграничения доступа к объектам, которые такую информацию содержат, в пределах этих групп. С учетом сказанного выше о различной архитектуре ППС и различных видах представления ИО, содержащих ИсОД и подлежащих защите, можно утверждать, что, согласно требованиям "Правил" и НД ТЗИ 2.5-008-2002, в ИС на базе ЛВС подлежат защите:

- в ИС с файл-серверной архитектурой ППС:
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии хранения в каталогах файловой системы серверов ИС (далее – О.СЛС.ХР.СЕРВ);
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии хранения в каталогах файловой системы рабочих станций ИС (далее – О.СЛС.ХР.РС);
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии обработки в клиентских ППС на рабочих станциях ИС (далее – О.СЛС.ОБР.РС);
- В ИС с 2-х уровневой клиент-серверной архитектурой ППС:
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии хранения в каталогах файловой системы серверов ИС (далее – О.СЛС.ХР.СЕРВ);
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии хранения в каталогах файловой системы рабочих станций ИС (далее – О.СЛС.ХР.РС);
  - ИО в виде сильносвязанных объектов, находящиеся в состоянии хранения в хранилищах данных серверов приложений (серверов СУБД) на серверах ИС (далее – О.СИЛС.ХР.ССУБД);

  - ИО в виде сильносвязанных объектов, находящиеся в состоянии обработки в ППС серверов приложений (серверов СУБД) на серверах ИС (далее – О.СИЛС.ОБР.ССУБД);
  - ИО в виде сильносвязанных объектов, находящиеся в состоянии обработки в клиентских ППС на рабочих станциях ИС (далее – О.СИЛС.ОБР.РС);
- В ИС с 3-х уровневой клиент-серверной архитектурой ППС:
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии хранения в каталогах файловой системы серверов ИС (далее – О.СЛС.ХР.СЕРВ);
  - ИО в виде слабосвязанных объектов, находящиеся в состоянии хранения в каталогах файловой системы рабочих станций ИС (далее – О.СЛС.ХР.РС);
  - ИО в виде сильносвязанных объектов, находящиеся в состоянии хранения в хранилищах данных серверов СУБД на серверах ИС (далее – О.СИЛС.ХР.ССУБД);
  - ИО в виде сильносвязанных объектов, находящиеся в состоянии обработки в ППС серверов СУБД на серверах ИС (далее – О.СИЛС.ОБР.ССУБД);
  - ИО в виде сильносвязанных объектов, находящиеся в состоянии обработки в ППС серверов приложений на серверах ИС (далее – О.СИЛС.ОБР.СПРИЛ);
  - ИО в виде сильносвязанных объектов, находящиеся в состоянии обработки в клиентских ППС на рабочих станциях ИС (далее – О.СИЛС.ОБР.РС).

Результаты анализа в обобщенном виде приведены в табл. 1.

Таблица 1 – Обобщенные требования по защите ИсОД в ИС на базе ЛВС

Задачи защиты	ФУБ	Тип, вид представления и состояние ИО, подлежащих защите в рамках политики соответствующих ФУБ		
		В ИС с файл-серверной архитектурой ППС	В ИС с двухуровневой архитектурой ППС	В ИС с трехуровневой архитектурой ППС
З.ОЗН.ПР, З.УРП.НД, З.АДМ.НД	КА-2	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС О.СИЛС.ХР.ССУБД О.СИЛС.ОБР.ССУБД О.СИЛС.ОБР.СПРИЛ О.СИЛС.ОБР.РС
З.МОД.ПР, З.ЦЕЛ.НД	*ЦА-2,* *ЦО-1*	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.СПРИЛ, О.СИЛС.ОБР.РС
З.КОП.ПР, З.КОП.НД	КА-2, *КО-1*	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС
З.АДМ.ПР, З.АДМ.НД	*НО-2*	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.СПРИЛ, О.СИЛС.ОБР.РС
З.АУТ.ПР, З.АУТ.НД	НИ-2, НК-1			
З.ДОСТ.ПР, З.ДОСТ.НД	*ДР-1*	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.СПРИЛ, О.СИЛС.ОБР.РС
З.ДОСТ.ПР, З.ДОСТ.НД	*ДС-1,* *ДЗ-1,* *ДВ-1*			

З.РЕГ.ПР, З.УЧ.НД, З.РЕГ.НД	*НР-2*	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС, О.СИЛС.ХР.ССУБД, О.СИЛС.ОБР.ССУБД, О.СИЛС.ОБР.СПРИЛ, О.СИЛС.ОБР.РС
З.АНРЕГ.ПР, З.КОНТР.НД	*НР-2*			
З.ЦЕЛПО.ПР	ЦА-2	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС	О.СЛС.ХР.СЕРВ, О.СЛС.ХР.РС
З.ЦЕЛКСЗ.ПР	НЦ-2, НТ-2			

Как видно из табл. 1, задачи защиты, которые должны реализовываться КСЗ в рамках политики соответствующих ФУБ, можно условно разделить на три части:

- основные задачи защиты и ФУБ, реализуемые по отношению к защищаемым ИО в виде как слабосвязанных, так и сильносвязанных объектов, находящимся как в состоянии хранения, так и в состоянии обработки (З.ОЗН.ПР, З.УРП.НД, З.АДМ.НД, З.МОД.ПР, З.ЦЕЛ.НД, З.АДМ.ПР, З.АДМ.НД, З.ДОСТ.ПР, З.ДОСТ.НД, З.РЕГ.ПР, З.УЧ.НД, З.РЕГ.НД);
- основные задачи защиты и ФУБ, реализуемые по отношению к ИО, представленным в виде только слабосвязанных объектов и находящимся в состоянии хранения (З.КОП.ПР, З.КОП.НД, З.ЦЕЛПО.ПР);
- вспомогательные задачи защиты и ФУБ, реализуемые безотносительно к виду представления и состоянию ИО (З.АУТ.ПР, З.АУТ.НД, З.ДОСТ.ПР, З.ДОСТ.НД, З.АНРЕГ.ПР, З.КОНТР.НД, З.ЦЕЛКСЗ.ПР).

Для того, чтобы определиться с возможностью реализации указанных задач штатными средствами защиты, реализованными в составе ОС семейства MS Windows, а также средствами защиты, реализованными в составе ППС ИС, проанализируем возможности этих средств. В составе ОС семейства MS Windows реализованы штатные средства защиты, основными функциями которых (при функционировании в составе ЛВС) являются идентификация и аутентификация пользователей, разграничение доступа пользователей к защищаемым ресурсам, уничтожение остаточной информации, а также регистрация и аудит связанных с безопасностью событий. Штатные средства разграничения доступа ОС семейства MS Windows построены в соответствии с концепцией диспетчера доступа (Reference Monitor) [8, 9]. Диспетчер доступа – компонент ОС, который реализует функции защиты информации путем: управления созданием активных объектов (пользователей и процессов) и пассивных объектов (источников/приемников информации в виде файлов данных или объектов типа каталог, служба, принтер, раздел реестра, совместно используемый объект, процесс, поток, задача, семафор, событие, мьютекс, проекция файла, ожидающий таймер, маркер, канал, оконная станция, рабочий стол и т. п.); предоставления пользователям и процессам доступа к пассивным объектам в соответствии с информацией, которая хранится в базе данных (БД) авторизации; уничтожения остаточной информации, которая содержится в удаленных пассивных объектах; регистрации событий (действий активных объектов) в БД регистрации. Управление БД авторизации (атрибутами доступа объектов) осуществляется пользователями на основании права владения этими объектами, управление настройками политики безопасности, БД учетных записей (атрибутами доступа пользователей) и БД регистрации осуществляется только пользователями, которые имеют соответствующие привилегии – администраторами. Привилегии могут также назначаться отдельным процессам.

Согласно с зарегистрированными Администрацией Госспецсвязи Экспертными заключениями № 150 от 24 сентября 2008 г., № 334 от 23 декабря 2011 г. и № 337 от 29 декабря 2011 г.:

- штатные средства защиты ОС Microsoft Windows XP Professional Service Pack 2 реализуют такой функциональный профиль защищенности: {КД-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-2, ДР-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1, НА-1, НП-1};
- штатные средства защиты ОС Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 реализуют такой функциональный профиль защищенности: {КД-2, КВ-1, КО-1, ЦД-1, ЦВ-1, ЦО-1, ДР-1, ДС-1, ДЗ-2, ДВ-2, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1};
- штатные средства защиты ОС Microsoft Windows 7 Enterprise Edition Service Pack 1 реализуют такой функциональный профиль защищенности: {КД-2, КВ-1, КО-1, ЦД-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1}.

Анализ перечня ФУБ, содержащихся в приведенных функциональных профилях защищенности, а также анализ политики соответствующих ФУБ [10] позволяет сделать следующие выводы:

- штатные средства ОС семейства MS Windows не могут быть использованы для реализации никакой из основных задач защиты, приведенных в табл. 1, по отношению к защищаемым ИО в виде как слабосвязанных, так и сильносвязанных объектов как в состоянии хранения, так и в состоянии обработки;
- штатные средства ОС семейства MS Windows не могут быть использованы для реализации вспомогательных задач защиты, приведенных в табл. 1, безотносительно к виду представления и состоянию ИО, поскольку решение указанных задач имеет смысл только в случае наличия возможности решения этими средствами основных задач защиты.

Что касается возможностей средств защиты, реализованных в ППС ИС, то, прежде всего, необходимо отметить, что в системах различной архитектуры (особенно это справедливо для ППС двухуровневой и трехуровневой архитектуры, а также обрабатываемых в них ИО в виде сильносвязанных объектов) как сами ИО, так и их атрибуты сохраняются в хранилищах данных ППС, построенных на базе серверов СУБД, а обрабатываются в программных средствах серверах приложений. С учетом того, что современные промышленные СУБД и инструментальные средства разработки приложений не налагают никаких существенных ограничений ни на перечень атрибутов, которые могут быть связаны с соответствующими ИО, ни на правила обработки этих атрибутов, которые могут быть реализованы, можно сделать следующие выводы:

- средства защиты, реализованные в ППС ИС, могут быть успешно (при условии получения необходимых атрибутов от средств, функционирующих на уровне ОС) использованы для реализации всех основных задач защиты, приведенных в табл. 1, но только по отношению к защищаемым ИО в виде сильносвязанных объектов как в состоянии хранения, так и в состоянии обработки;
- средства защиты, реализованные в ППС ИС, могут быть успешно (при условии получения необходимых атрибутов от средств, функционирующих на уровне ОС) использованы для частичной реализации вспомогательных задач защиты, приведенных в табл. 1, в той части, в которой решение этих задач возможно на уровне ППС, используемых для обработки ИО в виде сильносвязанных объектов;
- средства защиты, реализованные в ППС ИС, не могут быть использованы для реализации никакой из основных задач защиты, приведенных в табл. 1, по отношению к защищаемым ИО в виде слабосвязанных объектов как в состоянии хранения, так и в состоянии обработки;
- средства защиты, реализованные в ППС ИС, не могут быть использованы для реализации никаких вспомогательных задач защиты, приведенных в табл. 1, по отношению к защищаемым ИО в виде слабосвязанных объектов как в состоянии хранения, так и в состоянии обработки, поскольку решение указанных задач имеет смысл только в случае наличия возможности решения этими средствами основных задач защиты по отношению к ИО в соответствующем виде представления.

На основании приведенных результатов можно сделать вывод о том, что обеспечить защиту ИсОД в ИС на базе ЛВС в соответствии с требованиями действующего законодательства, используя только средства защиты, реализованные в ППС ИС и в ОС семейства MS Windows, невозможно. Для этого должны создаваться интегрированные КСЗ, в составе которых обязательно должны использоваться средств защиты, функционирующие на уровне ядра ОС (интегрированные в состав ОС) и обеспечивающие:

- решение основных задач защиты, приведенных в табл. 1, по отношению к защищаемым ИО в виде слабосвязанных объектов как в состоянии хранения, так и в состоянии обработки;
- решение вспомогательных задач защиты, приведенных в табл. 1, по отношению к защищаемым ИО в виде слабосвязанных объектов как в состоянии хранения, так и в состоянии обработки;
- взаимодействие со средствами защиты, реализованными в ППС ИС, с целью обеспечения поддержки решения основных и вспомогательных задач по отношению к защищаемым ИО в виде сильносвязанных объектов, а также обеспечения непрерывности защиты.

При этом в процессе взаимодействия средств защиты, реализованных в ППС ИС, со средствами защиты, интегрированными в состав ОС, как минимум, должна быть обеспечена возможность:

- передачи в средства защиты, реализованные в ППС ИС (с целью поддержки реализации задач защиты З.ОЗН.ПР, З.УРП.НД, З.МОД.ПР, З.ЦЕЛ.НД, З.КОП.ПР, З.УЧ.НД, З.АДМ.ПР, З.АДМ.НД, З.ДОСТ.ПР, З.ДОСТ.НД, З.РЕГ.ПР, З.УЧ.НД, З.РЕГ.НД), идентификаторов пользователей, зарегистрированных в каталоге пользователей ОС, а также их атрибутов доступа (уровня допуска к ИсОД, полномочий на выполнение операций импорта/экспорта, полномочий на выполнение операций печати и т. п.);

- передачи в средства защиты, реализованные в ППС ИС (с целью поддержки реализации задач защиты З.АУТ.ПР, З.АУТ.НД), идентификаторов пользователей, аутентифицированных средствами защиты, интегрированными в состав ОС, с целью их однозначной идентификации в ППС ИС;
- передачи в средства защиты, реализованные в ППС ИС (с целью поддержки реализации задач защиты З.ОЗН.ПР, З.УРП.НД, З.КОП.ПР, З.КОП.НД), атрибутов доступа импортируемых в ППС или экспортируемых из ППС ИО в виде слабосвязанных объектов с целью обеспечения контроля соответствия атрибутов доступа ИО (уровня конфиденциальности и т. п.) защищенных ИО в виде сильносвязанных объектов и являющихся основой для их создания (при импорте) или создаваемых на их основе (при экспорте) защищенных ИО в виде слабосвязанных объектов.

Рассмотрим возможность использования в качестве средств защиты, интегрированных в состав ОС, средств комплекса "Гриф" (Экспертное заключение № 239 от 13 августа 2010 г.) и комплекса "Гриф-Мережа" (Экспертное заключение № 203 от 24 декабря 2009 г.) производства ООО "Институт компьютерных технологий".

Комплекс "Гриф" может быть применен для защиты ИсОД, обрабатываемой на серверах и рабочих станциях одноранговой ЛВС, а комплекс "Гриф-Мережа" – для защиты ИсОД, обрабатываемой на серверах и рабочих станциях ЛВС с выделенным сервером – контроллером домена. При использовании на серверах и рабочих станциях ЛВС средства защиты, реализованные в составе комплексов "Гриф" и "Гриф-Мережа", реализуют:

- идентификацию и аутентификацию пользователей на основании имени (псевдонима), пароля и носителя данных аутентификации;
- разграничение обязанностей пользователей и выделение нескольких ролей администраторов, которые могут выполнять различные функции по администрированию (регистрацию защищаемых ресурсов, регистрацию пользователей, назначение прав доступа, обработку протоколов аудита и т. п.);
- разграничение доступа пользователей к выбранным каталогам (папкам) файловой системы и содержащимся в них ИО в виде слабосвязанных объектов (файлам данных), что позволяет организовать совместную работу нескольких пользователей, ИсОД;
- управление потоками информации и блокировку потоков информации, приводящих к снижению ее уровня конфиденциальности;
- контроль за выводом информации на печать с возможностью маркирования печатных листов выводимых документов (в формате "Office Open XML") согласно требованиям действующих нормативных документов в области охраны государственной тайны;
- контроль за экспортом информации на съемные носители с возможностью ограничения перечня используемых съемных носителей;
- контроль за импортом информации со съемные носителей;
- гарантированное удаление ИсОД путем затирания содержимого файлов при их удалении;
- разграничение доступа прикладных программ к выбранным каталогам (папкам) файловой системы и содержащимся в них ИО в виде слабосвязанных объектов (файлам данных), что позволяет обеспечить защиту ИсОД от случайного удаления или модификации и соблюсти технологию ее обработки;
- контроль целостности прикладного программного обеспечения и программного обеспечения комплекса, а также блокировку загрузки программ, целостность которых нарушена, что позволяет обеспечить защиту от вирусов и соблюдение технологии обработки ИсОД;
- контроль за использованием дискового пространства пользователями (квоты), что исключает возможность блокирования одним из пользователей возможности работы других;
- возможность блокировки устройств интерфейса пользователя (клавиатуры, мыши, монитора) на время его отсутствия;
- контроль целостности и самотестирование комплекса при старте;
- восстановление функционирования комплекса после сбоев, что гарантирует доступность информации при соблюдении правил доступа к ней;
- регистрацию, анализ и обработку информации о критичных для безопасности событиях (входа пользователя в ОС, попыток несанкционированного доступа, фактов запуска программ, работы с ИсОД, импорта/экспорта информации, вывода на печать и т. п.), что позволяет администраторам контролировать доступ к ИсОД, следить за тем, как используется комплекс, а также правильно его конфигурировать;
- ведение архива зарегистрированных данных аудита.

В составе комплексов реализованы специальные программные компоненты, предназначенные для организации взаимодействия со средствами защиты, реализованными в составе ППС ИС, в ходе функционирования интегрированных КСЗ.

В соответствии с Экспертными заключениями: средства комплексов реализуют политику административного управления доступом к ИсОД, а реализуемые ими функциональные профили защищенности ({КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НИ-3, НК-1, НО-2, НЦ-2, НТ-2} для комплекса "Гриф"; {КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2} для комплекса "Гриф-Мережа") соотвутствуют требованиям НД ТЗИ 2.5-008-2002..

Использование комплексов "Гриф" и "Гриф-Мережа" дает возможность реализовать действительно интегрированные КСЗ, обеспечивающие непрерывную защиту ИсОД, обрабатываемой в ИС. В качестве примера успешной реализации такого интегрированного КСЗ можно назвать КСЗ информационно-аналитической системы "Кадры ЗИ" версии 7.2. ППС системы "Кадры ЗИ" представляют собой программный комплекс двухуровневой клиент-серверной архитектуры, ориентированный на поддержку процессов автоматизации ведения кадрового учета в органах – субъектах властных полномочий. Информационная технология, реализованная в системе "Кадры ЗИ", обеспечивает: начальный ввод информации из первоисточников и ее коллективное использование; удобный интерфейс пользователей для доступа к информации с возможностью получения справок и построения списков; возможность получения пользователем оперативной текстовой и статистической информации.

Функционально система "Кадры ЗИ" состоит из таких подсистем: подсистемы ведения штатного расписания; подсистемы ведения личных карточек; подсистемы контроля качества заполнения данных; подсистемы генерации отчетов; поисковой подсистемы; подсистемы ведения классификаторов; подсистемы экспорта/импорта личных карточек, классификаторов, статистической отчетности и т.п.; подсистемы администрирования.

Структурно ППС системы "Кадры ЗИ" представляют собой совокупность программных модулей, которые функционируют на рабочих станциях ИС и на сервере СУБД (который, таким образом, одновременно выполняет функции сервера приложений). ППС системы, функционирующие на сервере СУБД (Oracle Server 9.2 или выше), реализованы в виде совокупности процедур и триггеров, которые сохраняются в соответствующем хранилище СУБД и выполняются в среде сервера СУБД. ППС системы, функционирующие на рабочих станциях ИС, представляют собой совокупность автоматизированных рабочих мест (АРМ) системы. Каждое АРМ представляет собой клиентское приложение Oracle, которое реализует функции, связанные с вводом/модификацией/просмотром/обработкой введенных данных, взаимодействием с сервером СУБД, а также специализированными программными средствами, реализующими функции просмотра/редактирования текстов документов и отчетов. В системе "Кадры ЗИ" может обрабатываться открытая информация, конфиденциальная информация, находящаяся в собственности субъектов властных полномочий (в т. ч персональные данные), и служебная информация.

Интегрированный КСЗ системы "Кадры ЗИ" включает в себя средства КСЗ "Гриф" версии 3.хх или КСЗ "Гриф-Мережа" версии 2.хх, а также средства защиты, реализованные в составе ППС системы. Согласно Экспертному заключению № 344 от 29 февраля 2012 г., КСЗ системы "Кадры-ЗИ" соответствует требованиям нормативных документов системы технической защиты информации в Украине, в т. ч. НД ТЗИ 2.5-008-2002, и может использоваться для защиты служебной информации и конфиденциальной информации, требования к защите которой установлены законом (информации с ограниченным доступом о физических лицах). Успешная реализация КСЗ системы "Кадры ЗИ" является практическим подтверждением правильности подходов, предложенных в данной статье.

В настоящее время в процессе реализации находится еще несколько интегрированных КСЗ, предназначенных для защиты ИсОД в ППС различного назначения (системах электронного документооборота, контроля исполнения поручений и т. п.).

Литература: ***1.*** *НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.* ***2.*** *НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***3.*** *Закон України "Про інформацію".* ***4.*** *Закон України "Про доступ до публічної інформації".* ***5.*** *Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".* ***6.*** *Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373.* ***7.*** *НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.* ***8.*** *Кастер Х. Основы Windows NT и NTFS/ Пер. с англ. – М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd.", 1996. – 440 с.* ***9.*** *Microsoft Windows Common Criteria Evaluation. Microsoft Windows 7. Microsoft Windows 2008 R2. Security Target, Version 1.0, March 23, 2011. http://www.commoncriteriaportal.org/products/.* ***10.*** *Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Технічні вимоги. http://www.microsoft.com/Ukraine/Security/Expert/.*