одноклассников) или klipz.ru (клипы). Соответственно политика безопасности на предприятии, и конкретная ее реализация на прокси-сервере требует корректировки.

Наличие сайта www.download.windowsupdate.com (обновления операционных систем разработки Microsoft corp.) в перечне целевых сайтов, указывает на необходимость создания локального корпоративного сайта обновлений программного обеспечения фирмы Microsoft для минимизации трафика. Либо может потребовать обращения внимания администратора сети на сетевые ПК, неподключенные к локальному серверу обновлений, так как ПК с необновляемой с необходимой периодичностью операционной системой могут оказаться узким местом безопасности корпоративной сети.

Причины возникновения инцидентов:

- несвоевременные обновления антивирусных баз данных, либо появление новых видов программного обеспечения, ведущего несанкционированную деятельность, и не являющегося вирусным ПО;
- использование внешних носителей информации (дискеты, flash-диски), как источников заражения;
- подключение к сети Интернет внутренних пользователей КСПИ;
- человеческий фактор.

Заключение:

Используемые технологии, являются в настоящее время эффективным средством защиты информации.

Методы защиты: совершенствование политики безопасности.

Список литературы

1.2007 CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com/forms/csi_survey.jhtml

2. Хорошко В.А., Чекатков А. А. Методы и средства защиты информации/Под. ред. Ю.С. Ковтанюка. - К.:Юниор, 2003.- 504 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-К.:ООО «ДС», 2001.-688 с.
4. В.А. Хорошко проф., д.т.н., С.А. Печень. Прикладные аспекты современных сетевых нефизических парольных атак и парольной защиты// Захист інформації, Спецвипуск, 2007 – с.88-94

Поступила 3. 03.2008г.

УДК.681.3.06(075)

С.Р.Коженевский, С.А.Чеховский

СПОСОБ ПОСТРОЕНИЯ ЗАЩИЩЕННОЙ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ОСНОВАННЫЙ НА МОДУЛЬНОМ ПРИНЦИПЕ

Построение локальной вычислительной сети с защитой информации от утечек по каналам ПЭМИН представляет собой сложную техническую задачу. Для решения этой задачи, в отличие от задачи защиты одиночного ПК, необходимо обеспечить экранирование всех элементов локальной сети - серверов и рабочих станций, активного и пассивного сетевого оборудования, распределенных в пространстве на значительные расстояния. Кабельная система локальной сети, как правило, выполненная на основе витой пары (экранированной либо неэкранированной), выполняет роль антенной системы для паразитных излучений элементов ПК и активного сетевого оборудования, эффективность и диаграмма

НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №3, 2008

ЗМІСТ

направленности которой зависит от взаимного расположения элементов сети, металлических систем (кабели, системы отопления, арматура в железобетоне) и пространственной конфигурации кабелей. При этом практически невозможно провести ни предварительные лабораторные исследования, ни объектовые измерения. Поэтому защищенные локальные сети на базе витой пары не нашли широкого применения.

При использовании оптоволоконных кабелей отсутствуют электромагнитные паразитные излучения кабеля и гальваническая связь между элементами локальной сети. Это упрощает решение задачи построения защищенной локальной сети и, в частности, упрощает требования к построению системы заземления и объектовым измерениям. Однако, сохраняется и ряд недостатков, связанных с дальнейшей эксплуатацией такой сети.

Кроме того, отсутствие общепринятых методик построения таких сетей и методик оценки уровней их защищенности, требует разработки и внедрения частных методик в каждом конкретном случае, что является сдерживающим фактором для их широкого применения.

Предлагается способ построения защищенной локальной сети для обработки конфиденциальной информации, основанный на модульном принципе. Основой для построения такой локальной сети является разработанный компанией ЕПОС специальный модуль - технический комплекс обработки конфиденциальной информации (ТК ОКИ).

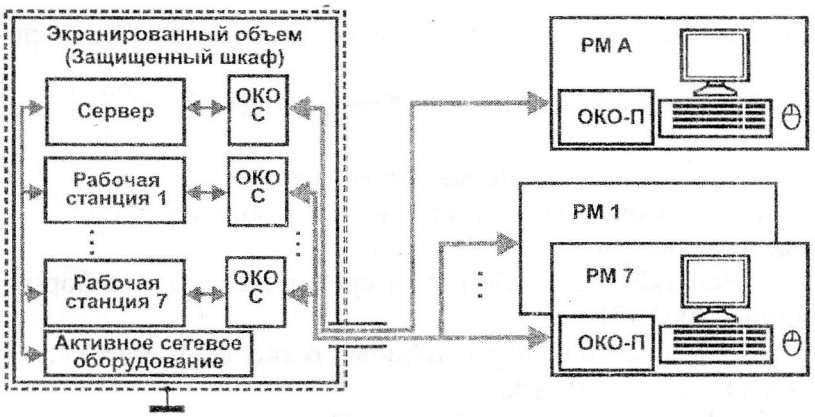

Рис.1 Базовый модуль защищенной локальной сети (ТК ОКИ)
РМ А – рабочее место администратора
РМ 1 – РМ 7 – рабочие места операторов

ТК ОКИ (рис.1) – специальный автономный модуль, представляющий собой сегмент защищенной локальной вычислительной сети (ЛВС), в котором обрабатываемые данные защищены от утечки по техническим каналам в соответствии с требованиями НД ТЗИ. Комплекс предназначен для создания автоматизированных систем класса 2, в которых обрабатывается информация с ограниченным доступом второй или третьей категории.
Базовый модуль ТК ОКИ включает в себе следующие технические средства:

- шкаф 19" со средствами технической защиты и с подавлением электромагнитного излучения и наводок,
- персональные компьютеры и/или сервера (всего до 8 шт. в одном шкафу),
- активное и пассивное оборудование локальной сети,
- специальные удаленные консоли оператора (LCD монитор, клавиатура, мышь с оптическими интерфейсами) разработки компании ЕПОС,
- специальные оптоэлектронные преобразователи "ОКО-С", "ОКО-П" (рис.2) разработки компании ЕПОС и оптоволоконные линии связи.

Рис.2. Специальные птоэлектронные преобразователи
«ОКО-С» и «ОКО-П»

При необходимости рабочие места могут оборудоваться периферийным оборудованием (принтеры, сканеры...).

Такие модули могут объединяться в единую автоматизированную систему без ограничения требуемого количества рабочих мест.

Принцип технической защиты информации

основан на том, что весь сегмент локальной сети (системные блоки ПК, сервер и оборудование ЛВС) размещается в специальном экранированном шкафу, который обеспечивает защиту данных от утечки по каналам ПЭМИН, защиту информации от разрушения внешним электромагнитным воздействием и от несанкционированного физического доступа к ней. При этом на рабочих местах операторов размещается только удаленная консоль в защищенном исполнении (монитор, клавиатура и манипулятор-мышь), которая с помощью специальных оптоэлектронных преобразователей "ОКО" подключается оптоволоконными линиями к системным блокам в шкафу.

При такой схеме подключения оператор на рабочем месте не имеет физического доступа к системному блоку, установленного в шкафу. Шкаф оснащен системой сигнализации и кодовым замком, что позволяет решать организационно-техническими мерами вопросы хранения информации с ограниченным доступом непосредственно в шкафу.

Ввод и вывод данных с рабочего места оператора может осуществляться посредством сменного флэш-накопителя через порт USB на консоли оператора. При необходимости контролирования (например, офицером безопасности) таких операций ввода-вывода информации, порт USB, размещается только в системном блоке в шкафу.

Аутентификация пользователя осуществляется при помощи смарт-карты, которая вставляется в считыватель, размещенный на консоли оператора.

Варианты защищенной локальной сети на базе ТК ОКИ:

1. Автоматизированная система класса 2 для одной рабочей группы с числом автоматизированных рабочих мест до 8.

В этом случае используется один модуль. Рабочие места могут размещаться как в одном помещении, так и в разных комнатах или на разных этажах. Максимальное расстояние удаления консоли оператора от шкафа с компьютерным оборудованием 100 м. На таких же расстояниях от шкафа может быть размещено и дополнительное оборудование. Локальная сеть может быть с выделенным сервером (сервер и до 7 шт. ПК) или одноранговой (до 8 шт. ПК)

2. Автоматизированная система класса 2 с неограниченным числом автоматизированных рабочих мест.

Количество пользователей в автоматизированной системе можно увеличить, если объединить несколько технических комплексов (модулей) в единую структуру. Для этого в защищенный шкаф одного из модулей устанавливается оптический коммутатор, к которому при помощи высокоскоростных оптоволоконных линий связи подключаются соседние модули. Количество подключаемых модулей практически не ограничено. При территориально распределенной структуре автоматизированной системы расстояние между модулями может составлять несколько километров.

Поскольку каждый модуль обладает стабильными электромагнитными характеристиками, на которые соседние модули не оказывают влияния, существует возможность поэтапного создания автоматизированной системы с большим количеством рабочих мест. При этом после каждого шага наращивания (подключения дополнительного модуля) специальные исследования по ТЗИ проводятся не для всей системы, а только для нового модуля.

Внедрение компанией ЕПОС модульного принципа при построении защищенных локальных сетей на базе ТК ОКИ в ряде организаций позволило снизить сроки ввода в эксплуатацию защищенных сетей, ограничить несанкционированный доступ к конфиденциальной информации и снизить эксплуатационные затраты. Такой принцип построения защищенных сетей с нашей точки зрения может явиться основой для разработки общепринятых методик построения и оценки уровня их защищенности в общегосударственном масштабе.

Поступила 26.03.2008г.

УДК 004.056:378(147)

М.Г.Коляда

ПРОГНОЗУВАННЯ ОБСЯГІВ ПЕРЕДАЧІ ЗАХИЩЕНОЇ ІНФОРМАЦІЇ ПО РАДІОКАНАЛАХ НА ОСНОВІ ТЕОРІЇ ГРИ З ПРИРОДОЮ

Вступ

Останнім часом затребуваність знань з теорії ігор у різних прикладних областях людської діяльності підсилюється

Теорія ігор усе ширше проникає в практику прогнозування економічних процесів. Її можна розглядати як інструмент, що допомагає підвищити ефективність планових і управлінських рішень. Вона знайшла широке застосування в області створення інтелектуальних ігрових та навчальних систем.

Однак при використанні теорії ігор, варто пам'ятати про особливості, які існують при застосуванні цієї теорії в області захисту інформації. Деякі автори [1] указують, що міні-максна теорія стратегічних ігор не завжди є найкращим підходом при моделюванні систем захисту. Як відомо міні-максна стратегія припускає, що функція $\varphi(p)$ супротивника -- протилежність вашої власної функції $\varphi(s)$. Таким чином, $\varphi(p) = -\varphi(s)$. В області економіки і менеджменту подібне допущення мало деякий успіх. Однак, в області побудови систем захисту інформації таке припущення не завжди справедливе, тому що мається ряд причин при яких $\varphi(s) \neq \varphi(p)$. Насамперед, зловмисник, цілком ймовірно, має мету відмінну від цілей і пріоритетів системи захисту. По-друге, далеко не завжди зловмисник має повну інформацію щодо конфігурації системи захисту, що значно ускладнює для нього можливість судити наскільки він близько знаходиться біля своїх цілей.

Іншою негативною стороною застосування теорії ігор в питаннях захисту інформації є те, що існують обмеження в можливостях автоматизованої розробки рівноважної (цільової) функції. У початковій стадії розвитку цієї ідеї було все добре; були розроблені методології для настроювання таких рівноважних функцій протягом гри. Найбільш яскравим прикладом, служить використання нейронних мереж у боротьбі з мережними атаками.

На відміну від експертних систем, які можуть дати користувачу визначену відповідь, чи відповідають чи ні поточні характеристики, еталонним характеристикам, які закладено у базу цих правил, нейромережа аналізує інформацію і оцінює, чи погодяться дані, які розглядаються з характеристиками, які вона повинна розпізнати. Відомо, що спочатку нейромережа сама навчається шляхом правильної ідентифікації попередньо обраних прикладів предметної області. Реакція